Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Armed Forces Academy of General Milan Rastislav Štefánik

ZBORNÍK PRÍSPEVKOV
z 13. medzinárodnej vedeckej konferencie

Proceedings of the International Conference on National and International Security

20th - 21st October 2022 • Liptovský Mikuláš • Slovakia

NMB

NÁRODNÁ A MEDZINÁRODNÁ BEZPEČNOSŤ 2022

13. medzinárodná vedecká konferencia

NATIONAL AND INTERNATIONAL SECURITY 2022

13th International Scientific Conference

Zborník príspevkov
z medzinárodnej vedeckej konferencie

Proceedings of the International Conference
on National and International Security

NIS

20th - 21st October 2022 • Liptovský Mikuláš • Slovakia

Organizátor / Organizer

- Akadémia ozbrojených síl generála Milana Rastislava Štefánika
  Katedra bezpečnosti a obrany

Spoluorganizátori / Co-organizers

- Ministerstvo obrany Slovenskej republiky
- Generálny štáb OS SR
- Univerzita obrany Brno
- War Studies University Warsaw
- National University of Public Service Budapest
- APEIRON Academy of Security of Public and Individual Crakow
- Univerzita Mateja Bela Banská Bystrica
- Akadémia Policajného zboru Bratislava

Záštita / Auspices

- PhDr. Jaroslav NAĎ, PhD.

minister obrany Slovenskej republiky

Garanti / Guarantors

- doc. Ing. Jozef PUTTERA, CSc., rektor, Akadémia ozbrojených síl generála Milana Rastislava Štefánika Liptovský Mikuláš, Slovenská republika
- brig. gen. prof. RNDr. Zuzana KROČOVÁ, Ph.D., rektorka, Univerzita obrany Brno, Česká republikaa
- prof. JUDr. Lucia KURILOVSKÁ, PhD., rektorka, Akadémia Policajného zboru v Bratislave, Slovenská republika
- Dr Juliusz PIWOWARSKI, rektor, APEIRON Academy of Security of Public and Individual in Krakow, Poľská republika
- COL Dr. hab. Dariusz MAJCHRZAK, prorektor pre vojenské veci, War Studies University Warsaw, Poľská republika
- Brig. Gen. Dr. Árpád POHL, dekan, Faculty of Military Sciences and Officer Training, National University of Public Service Budapest, Maďarská republika
- doc. PhDr. Branislav KOVÁČIK, PhD., dekan, Fakulta politických vied a medzinárodných vzťahov Univerzity Mateja Bela v Banskej Bystrici, Slovenská republika
- prof. Ing. Vojtech JURČÁK, CSc., vedúci katedry bezpečnosti a obrany, Akadémia ozbrojených síl generála Milana Rastislava Štefánika Liptovský Mikuláš, Slovenská republika

Vedecký výbor / Scientific Committee

- doc. Ing. Lubomír BELAN, PhD., Akadémia ozbrojených síl generála Milana Rastislava Štefánika Liptovský Mikuláš, Slovenská republika
- prof. Ing. Martina BLAŠKOVÁ, PhD., Police Academy of the Czech Republic Prague, Czech Republic
- Ing. Daniel BREZINA, PhD., Akadémia ozbrojených síl generála Milana Rastislava Štefánika Liptovský Mikuláš, Slovenská republika
- COL Prof. Vasile CARUTASU, PhD., Land Forces Academy Sibiu, Romania
- Dr. Wojciech CZAJKOWSKI, APEIRON Cracow, Poland
- doc. Ing. Dr. Štefan DANICS, Ph.D., Police Academy of the Czech Republic Prague, Czech Republic

- Dr. Tomasz DUKIEWICZ, University of Opole, Opole, Poland
- doc. Ing. Boris ĎURKECH, CSc., Akadémia ozbrojených síl Liptovský Mikuláš, Slovenská republika
- COL Assoc. Prof. Sasho S. EVLOGIEV, PhD., Faculty Artillery, AD and CIS Shumen, Bulgaria
- MAJ. Tibor FARKAS, PhD., National University of Public Service, Budapest, Hungary
- PhDr. Libor FRANK, Ph.D., University of Defence Brno, Czech Republic
- COL Assoc. Prof. Eng. Laurian GHERMAN, PhD., Air Force Academy Braşov, Romania
- prof. PhDr. František HANZLÍK. CSc., University of Defence Brno, Czech Republic
- plk. gšt. v. z. doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc., Akadémia Policajného zboru v Bratislave, Slovenská republika
- doc. PhDr. Rastislav KAZANSKÝ, PhD., UMB v Banskej Bystrici, Slovenská republika
- COL prof. Klára S. KECSKEMÉTHY, PhD., National University of Public Service, Budapest, Hungary
- doc. Ing. Zbyšek KORECKI, Ph.D., University of Defence Brno, Czech Republic
- prof. Dr hab. Dariusz KOZERAWSKI, Jagiellonian University Krakow, Poland
- COL prof. Zoltan KRAJNC, PhD., National University of Public Service, Budapest, Hungary
- doc. Ing. Karel KUBEČKA, Ph.D., AMBIS Prague, Czech Republic
- doc. Ing. Ivan MAJCHÚT, PhD., Akadémia ozbrojených síl Liptovský Mikuláš, Slovenská republika
- prof. dr hab. Jan MACIEJEWSKI, Univerzity of Wroclaw, Poland
- prof. dr hab. Maciej MARSZAŁEK, War Studies University Warsaw, Poland
- ks. dr hab. Miroslaw A. MICHALSKI, WSB Toruň, Poland
- prof. Ing. Jana MŰLLEROVÁ, PhD. Akadémia Policajného zboru v Bratislave, Slovenská republika
- Assoc. Prof. Marijana MUSLADIN, Ph.D. - University of Dubrovnik, Dubrovnik, Croatia
- COL Dr. hab. inż. Jacek NARLOCH, Military Univerzity of Land Forces Wroclaw, Poland
- prof. Ing. Pavel NEČAS, PhD., UMB v Banskej Bystrici, Slovenská republika
- Assoc. Prof. Antoni OLAK, WSPA Lublin / PWSTE Jarosław, Poland
- gen. mjr. Ing. Ivan PACH, Pozemné sily OS SR, Slovenská republika
- COL dr. hab. Przemyslaw PAŻDZIOREK, War Studies University Warsaw, Poland
- Assoc. Prof. Elitsa PETROVA, DSc., National Military University Veliko Tarnovo, Bulgaria
- Dr hab. Andrzej PIECZYWOK, Kazimierz Wielky University Bydgoszcz, Poland
- doc. Ing. Ivo PIKNER, Ph.D., University of Defence Brno, Czech Republic
- doc. Ing. Josef PROCHÁZKA, Ph.D., University of Defence Brno, Czech Republic
- dr. hab. Adam RADOMYSKI, Polish Air Force University in Dęblin, Poland
- doc. Ing. Peter SPILÝ, PhD., Akadémia ozbrojených síl Liptovský Mikuláš, Slovenská republika
- Dr. hab. Henryk SPUSTEK, University of Opole, Opole, Poland
- Mgr. Richard STOJAR, Ph.D., University of Defence Brno, Czech Republic
- plk. Mgr. Ing. Pavel ŠVELKA, Sily pre špeciálne operácie OS SR, Slovenská republika
- dr. hab. inż. Norbert ŚWIĘTOCHOWSKI, Military Univerzity of Land Forces Wroclaw, Poland
- brig. gen. Ing. Róbert TÓTH, Vzdušné sily OS SR, Slovenská republika
- Assoc. Prof. Inga URIADNIKOVA, CSc., National poletechnical university Odessa, Ukraine
- doc. Mgr. Jaroslav UŠIAK, PhD., UMB v Banskej Bystrici, Slovenská republika

- doc. Ing. Jaroslav VARECHA, PhD., Akadémia ozbrojených síl Liptovský Mikuláš, Slovenská republika
- Assoc. Prof. Vasiľ ZAPLATINSKIJ, PhD. National Aviation University Kyiv, Ukraine
- COL (RES) Mariusz WOJCISZKO, Ph.D., War Studies University Warsaw, Poland

Organizačný výbor / Organizing Committee

- doc. Ing. Ivan MAJCHÚT, PhD. - predseda
- Ing. Daniel BREZINA, PhD.
- Katarína ERHARDTOVÁ
- npor. Mgr. Tatiana FÁBRYOVÁ
- JUDr. Tomáš MARTAUS
- npor. Martin ONDRUŠ
- Ing. Rudolf PÁSTOR
- kpt. Ing. Monika SAGANOVÁ
- Mgr. Juraj ŠIMKO, PhD.

Recenzenti / Reviewers

- doc. Ing. Lubomír BELAN, PhD.
- Ing. Daniel BREZINA, PhD.
- doc. Ing. Boris ĎURKECH, CSc.
- prof. Ing. Ladislav HOFREITER, CSc.
- prof. Ing. Vojtech JURČÁK, CSc.
- mjr. Ing. Jaroslav KOMPAN, PhD.
- doc. Ing. Ivan MAJCHÚT, PhD.
- PhDr. Mária MARTINSKÁ, PhD.
- doc. Ing. Stanislav MORONG, PhD.
- Ing. Rudolf PÁSTOR
- doc. PhDr. Mária PETRUFOVÁ, PhD.
- doc. Ing. Peter SPILÝ, PhD.
- Mgr. Juraj ŠIMKO, PhD.
- doc. Ing. Jaroslav VARECHA, PhD.

ISBN 978-80-8040-631-8

Akadémia ozbrojených síl gen. M. R. Štefánika
Katedra bezpečnosti a obrany
Armed Forces Academy of gen. M. R. Štefánik
Security and Defence Department

PROGRAM KONFERENCIE
CONFERENCE PROGRAM

13. Medzinárodná vedecká konferencia
13th International Scientific Conference

NÁRODNÁ A MEDZINÁRODNÁ BEZPEČNOSŤ 2022
NATIONAL AND INTERNATIONAL SECURITY 2022

20. - 21. 10. 2022

20. 10. 2022

13:30 – 13:40 Otvorenie konferencie / Conference opening
13:40 – 14:00 Vystúpenie pozvaných hostí / Performance of invited guests
Fotografovanie / Photography

14:00 – 15:20 Blok I: Medzinárodné vzťahy / International relations
Konferenčná miestnosť / conference room Moderator: Peter **SPILÝ**

Klára S. KECSKEMÉTHY National University of Public Service Budapest **Alexandra SIPOS** Centre for Social Sciences, Budapest	The Alliance´s partnerships in the light of the Madrid Summit
Péter SZITÁS National University of Public Service Budapest	The non involvement of Hungary in the war on Ukraine
Anna ĎURFINA VŠMaVV Praha	Eastern Europe reflected by the Copenhagen school of security

15:20 – 15:40 **Prestávka / break**

15:40 – 16:40 Blok II: Národná bezpečnosť / National security
Konferenčná miestnosť / conference room Moderator: Ladislav **HOFREITER**

Antonín NOVOTNÝ Univerzita obrany Brno	Strategický kompas Evropské unie – jeho implementace v České republice
Ivo PIKNER Univerzita obrany Brno	Přístupy k tvorbě operačních koncepcí
Petr KŘÍŽEK Univerzita obrany Brno	Pokročilé mobilizační plánování požadavek na urychlení rozvoje schopností ozbrojených sil

16:40 – 17:00 **Prestávka / break**

17:00 – 18:00 Blok III: Bezpečnostná veda / Security science
Konferenčná miestnosť / conference room Moderator: Rudolf **PÁSTOR**

Norbert ŚWIĘTOCHOWSKI Military University of Land Forces Wroclaw	War and Peace in Human Live
Marek HARGAŠ Akadémia ozbrojených síl Liptovský Mikuláš	Ciele a plánované dopady sankcií proti Rusku od začiatku invázie na Ukrajinu
Martin ONDRUŠ Akadémia ozbrojených síl Liptovský Mikuláš	Bezpečnostné prostredie a jeho dynamika
Peter POLÁČEK Akadémia ozbrojených síl Liptovský Mikuláš	Aplikácia informačnej bezpečnosti vo vesmírnom sektore z pohľadu NATO

19.00 - 22.00 **SPOLOČENSKÝ VEČER / SOCIAL PROGRAM**

21. 10. 2022

08:30 – 10:00 Blok IV: Použitie ozbrojených síl / Deployment of armed forces

Konferenčná miestnosť/ conference room Moderator: Daniel **BREZINA**

Tamás BEREK National University of Public Service Budapest	The role of commander's CBRN Expertise
Tibor FARKAS National University of Public Service Budapest	C4ISR for Command and Control
Zoltán KRAJNC National University of Public Service Budapest	Development of Air Defence Missile planning capabilities in University of Public Service
Ivan BYSTRIANSKY Akadémia ozbrojených síl Liptovský Mikuláš	Výcvikové zariadenie "OREMLAND"
Monika SAGANOVÁ Akadémia ozbrojených síl Liptovský Mikuláš	Odborná profesionalita dôstojníkov OS SR

10.00 - 10.15 **Prestávka/ break**

10:15 – 11:45 Blok V: Bezpečnostná veda – konšpiračné teórie / Security science – conspiracy theories

Konferenčná miestnosť/ conference room Moderator: Juraj **ŠIMKO**

Radoslav IVANČÍK Akadémia Policajného zboru Bratislava	Sociálne siete ako priestor pre šírenie konšpiračných teórií a dezinformácií
Dominika ČERNÁKOVÁ Ministerstvo obrany SR Bratislava	Kto je ochotný brániť Slovensko?
Róbert TOMÁŠEK Akadémia ozbrojených síl Liptovský Mikuláš	O hybridných hrozbách a hybridnej vojne
Tatiana FÁBRYOVÁ Akadémia ozbrojených síl Liptovský Mikuláš	Psychologické operácie
Marek DVOŘÁČEK Masarykova univerzita Brno	Contemporary Security Threats for Outer Space
Antoni OLAK WSPiA Lublin	Refugees and their Protection – Legal and International Aspects

11:45 – 13:00 Ukončenie konferencie/ Ending a conference
Obed/ Lunch

Za obsah a spôsob vystúpení zodpovedajú v plnom rozsahu autori.
The content and the way of the performance are in the responsibility of the authors.

OBSAH

KONFLIKT NA UKRAJINE A JEJ DOPAD NA BEZPEČNOSŤ EURÓPSKEJ ÚNIE

THE CONFLICT IN UKRAINE AND ITS IMPACT ON THE SECURITY OF THE EUROPEAN UNION

Martin BAKIČ

ABSTRACT

The events in Ukraine in 2014 significantly affected world geopolitics, including the geopolitical position of the Russian Federation. These events significantly influenced the status quo in the world and affected mutual relations and perceptions between the member states of the European Union and the Russian Federation, which has a fundamental impact on the international security environment in Europe.

The main objective of the article is to analyze and evaluate the consequences of the conflict in Ukraine and its impact on the security of the European Union from 2014 to 2022 and to answer following research questions. How has the defense policy and strategy of the European Union changed? What are the defense ambitions and investments of the European Union in cooperation with the North Atlantic Alliance? Is there a common perception of potential security threats among the member states of the European Union? How did the member states of the European Union react to the aggression of the Russian Federation and what security measures did the European Union adopt?

Keywords: defense, strategy, security, European Union

ÚVOD

John Mearsheimer profesor medzinárodných vzťahov na univerzite v Chicagu predpovedal, že situácia medzi Ukrajinou a Ruskou federáciou (ďalej len RF) je zrelá na to, aby medzi týmito krajinami došlo k súpereniu v bezpečnostnej oblasti. Veľké krajiny, ktoré majú dlhú a nechránenú spoločnú hranicu ako Ukrajina a RF, často skĺznu k súpereniu v obavách o svoju bezpečnosť. Ukrajina a RF by mohli túto tendenciu premôcť a žiť v harmónii, avšak pokiaľ sa im to podarí, bude to neobvyklé. (Huntington, 2001, s. 27)

Z pohľadu článku je tvrdenie Johna Mearsheimera na začiatku deväťdesiatich rokov varovným signálom pre Európu, jej mier a bezpečnosť. Udalosti na Ukrajine v roku 2014 výraznou mierou ovplyvnili svetovú geopolitiku, vrátane geopolitického postavenia RF. Tieto udalosti výraznou mierou zasiahli status quo vo svete a ovplyvnili vzájomné vzťahy a vnímania medzi členskými štátmi Európskej únie (ďalej len EÚ) a RF, čo má zásadný vplyv na medzinárodno-bezpečnostné prostredie v Európe.

Tento článok sa zameriava na hodnotenie dôsledkov konfliktu na Ukrajine a jej dopad na bezpečnosť EÚ. Analyzuje obdobie od vzniku konfliktu v roku 2014 až po nevyprovokovanú a neopodstatnenú vojenskú agresiu RF voči Ukrajine v roku 2022. Z výskumného hľadiska je potrebné v článku zodpovedať na nasledujúce otázky. Na základe udalostí na Ukrajine vyhodnotíme ako sa od roku 2014 zmenila obranná politika a stratégia EÚ. Aké sú obranné ambície a investície EÚ? Taktiež aj v spolupráci s NATO, ktoré kooperuje v euroatlantickom priestore. Existuje spoločné vnímanie potencionálnych bezpečnostných hrozieb medzi

členskými štátmi EÚ? Ako členské štáty EÚ zareagovali na agresiu RF a aké bezpečnostné opatrenia EÚ prijala?

Na vyvodenie konkrétnych záverov sme použili viaceré metódy. Faktorovou analýzou sme zhodnotili prijaté opatrenia a v zmysle výskumný otázok sme sformulovali záver v súvislosti s konfliktom na Ukrajine a jej dopad na bezpečnosť EÚ. Autor si nedáva za cieľ v článku analyzovať jednotlivé dôvody vzniku vojenského konfliktu na Ukrajine, prípadne rozoberať jeho priebeh.

1 ZAHRANIČNÁ POLITIKA EURÓPSKEJ ÚNIE

Medzinárodný vývoj a bezpečnostné hrozby, ktorým čelí EÚ od roku 2014 dodali európskej obrannej spolupráci novú hybnú silu. Bezpečnosť EÚ ohrozuje terorizmus, hybridné hrozby, ekonomická nestabilita, zmena klímy a energetická neistota. Cieľom EÚ je zvýšiť príspevok k európskej kolektívnej bezpečnosti úzkou spoluprácou so svojimi partnermi, počnúc NATO. Odolnosť štátov a spoločností na východ a na juh od EÚ chce presadzovať prostredníctvom investícií do odolnosti štátov a spoločností na východ až po Strednú Áziu a na juh až po strednú Afriku.

V súvislosti s bezpečnostnými hrozbami, ktoré ohrozujú EÚ bola v roku 2016 prijatá Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ (ďalej len Globálna stratégia). Jej hlavným zámerom v oblasti bezpečnosti a obrany je začatie niekoľkých iniciatív a mechanizmov. Globálna stratégia uvádza do popredia spoločné záujmy a princípy. Prioritou EÚ bude presadzovanie mieru a zaručenie bezpečnosti svojich občanov a územia. Domáca bezpečnosť EÚ súčasne závisí od mieru za hranicami EÚ. EÚ bude presadzovať globálny poriadok založený na pravidlách. Zodpovednosť si kladie nie len v rámci celej Európy ale aj vo vzťahoch so susediacimi regiónmi na východe a juhu. Cieľom EÚ je riešiť základné príčiny konfliktov, chudoby a presadzovať ľudské práva. EÚ bude zodpovedným globálnym aktérom, ale zodpovednosť musí byť spoločná. Zodpovednosť bude sprevádzaná reformami s vonkajšími partnerstvami. EÚ si kladie za cieľ oslovovať štáty, regionálne orgány a medzinárodné organizácie. Spolupracovať s kľúčovými partnermi, podobne zmýšľajúcimi krajinami a regionálnymi zoskupeniami. (SZBP, 2016)

Globálna stratégia reflektuje a očakáva, že väčšina rastu sa v blízkej budúcnosti uskutoční mimo EÚ. Prosperita sa bude čoraz viac opierať o obchod a investície. Prosperujúca Európa závisí od silného vnútorného trhu a otvoreného medzinárodného hospodárskeho systému. EÚ kladie dôraz predovšetkým na vieru v účinnosť medzinárodného práva, na narastajúcu úlohu medzinárodných inštitúcií, na vieru vo svet bez hraníc, v ktorom bude stále viac demokracie, mieru a slobody, ktoré budú smerovať k časom bez kríz a vojenských konfliktov.

O členstvo v EÚ môže požiadať každý európsky štát, teda aj Ukrajina. Politika EÚ voči kandidátskym krajinám bude naďalej vychádzať z jasného, prísneho a spravodlivého prístupového procesu. V prvom rade sa bude sústreďovať na základné požiadavky členstva a jej súčasťou bude prísnejšia kontrola reforiem. Podpora EÚ a spolupráca s týmito krajinami musí zároveň prinášať konkrétne výhody a musí sa dobre vysvetľovať. To znamená spoluprácu v oblasti boja proti terorizmu, reformy sektora bezpečnosti, migrácie, infraštruktúry, energetiky a klímy. Prehlbovanie medziľudských kontaktov a cielenú úpravu niektorých foriem pomoci EÚ s cieľom dosiahnuť zreteľné zlepšenie životných podmienok občanov.

Globálna stratégia uvádza do popredia ako najvýznamnejší vzťah zo všetkých krajín Východného partnerstva práve Ukrajinu. Geograficky a kultúrne je Ukrajina najbližšie. Ako súčasť Európskej susedskej politiky, Ukrajina s EÚ uzatvorila Asociačnú dohodu, ktorá je v platnosti od roku 2017. Súčasťou asociačnej dohody je tzv. prehĺbená a komplexná dohoda o zóne voľného obchodu (z angl. Deep and Comprehensive Free Trade Area - DCFTA)

a negociácia o vízovej liberalizácii. Hlavým cieľom Ukrajiny pre vstup do EÚ bude dodržiavanie a podporovanie hodnôt zakotvených v zmluvách EÚ. Dôveryhodná politika rozširovania musí byť založená na prísnej a spravodlivej podmienenosti. Dôveryhodná politika rozširovania predstavuje strategickú investíciu do bezpečnosti a prosperity Európy a v značnej miere už prispela k mieru v oblastiach, kde sa predtým konala vojna. (SZBP, 2016)

Porušovanie medzinárodného práva zo strany RF a jeho destabilizácia Ukrajiny sú spolu s dlhotrvajúcimi konfliktmi v širšom čiernomorskom regióne útokom na jadro európskeho bezpečnostného poriadku. EÚ si zakladá na princípoch a jednotnosti pri podpore medzinárodného práva, demokracie, ľudských práv, spolupráce a práva každej krajiny slobodne si zvoliť svoju budúcnosť.

Kľúčovou strategickou výzvou EÚ je riadenie vzťahov s RF. Základným cieľom politiky EÚ voči RF musí zostať jednotný a spoločný prístup. Podstatné zmeny vo vzťahoch medzi EÚ a RF sú podmienené úplným dodržiavaním medzinárodného práva a zásad podporujúcich európsky bezpečnostný poriadok vrátane Helsinského záverečného aktu a Parížskej charty. EÚ neuzná protiprávnu anexiu a destabilizáciu teritoriálnych území na Ukrajine zo strany RF. EÚ mieni posilniť, zvýšiť odolnosť východných susedov teda aj Ukrajiny a bude podporovať ich právo slobodne určiť svoj postoj k EÚ. Zároveň je potrebné poznamenať, že medzi EÚ a RF existuje vzájomná závislosť. Preto EÚ bude zapájať RF do rokovaní o nezhodách a spolupracovať s ním, tak aby sa záujmy prelínali. Kľúčové otázky zahraničnej politiky medzi EÚ a RF budú selektívne angažovať sa v oblastiach európskeho záujmu, námornej bezpečnosti, vzdelávania, výskumu a cezhraničnej spolupráce.

2 OBRANNÁ POLITIKA EURÓPSKEJ ÚNIE - JEJ AMBÍCIE A INVESTÍCIE

Podľa preskúmania Európskeho dvora audítorov z roku 2019, súčasné vojenské spôsobilosti a spolupráca členských štátov EÚ nezodpovedajú novej úrovni ambícií obrannej politiky EÚ. Dôležitú tézu zohrávajú synergie medzi iniciatívami EÚ a ostatnými obrannými a bezpečnostnými rámcami. Rozhodujúcou otázkou je, či EÚ bude schopná dopĺňať NATO a predchádzať duplicite a recipročnému prekrývaniu. Iniciatívy na úrovni EÚ a navrhované zvýšenie financovania predstavujú výkonnostné riziká. Členské štáty EÚ až do vzniknutého konfliktu na Ukrajine v roku 2014 prijímali v otázkach európskej obrany len obmedzené kroky. V reakcii na nové, náročné podmienky globálneho prostredia však EÚ spustila nové iniciatívy s cieľom posilniť spoluprácu medzi členskými štátmi. (EDA, 2019)

Obrana je oblasťou nerozlučne spätá s národnou zvrchovanosťou členských štátov EÚ. Do popredia sa vynára riziko strategických rozdielov medzi členskými štátmi EÚ v rámci ich vnímania bezpečnostných hrozieb a úlohy európskej obrany, ktoré sa môžu líšiť. V členských štátoch EÚ tiež platia odlišné pravidlá vojenského zapojenia a panujú rôznorodé pohľady na použitie vojenskej sily. Napríklad, niektoré členské štáty sa zameriavajú skôr na územnú obranu voči vojenským hrozbám zo strany RF (krajiny východnej Európy ako Lotyšsko, Litva, Estónsko a Poľsko), zatiaľ čo iné sa orientujú viac na bezpečnostné výzvy pochádzajúce zo severnej Afriky a Blízkeho východu (krajiny južnej Európy ako Španielsko a Taliansko). Niektoré členské štáty majú tradíciu neutrality, zatiaľ čo iné sú ochotné zúčastňovať sa aj širokospektrálnych operácií. Pre väčšinu členských štátov EÚ pozostáva európska obrana hlavne z dvoch dôležitých úrovní. Z vlastnej obrannej spôsobilosti členských štátov a z kolektívnej obrany zabezpečovanej prostredníctvom Aliancie. (EDA, 2019)

Juhan Parts člen Európskeho dvora audítorov zodpovedný za preskúmavanie plánov EÚ v oblasti obrany konštatuje:

- Obrana zahŕňa rozvoj reálnych vojenských spôsobilostí s jasným potenciálom odrádzať od prípadných hrozieb.

- Bez dôležitých faktorov úspechu a bez konkretizovania jasných cieľov existuje riziko, že súčasné iniciatívy EÚ v oblasti obrany zostanú prázdnym dokumentom a skončia bez výsledku.

Pokiaľ ide o obranu, existuje viditeľný rozpor medzi tým, čo sa od členských štátov očakáva, a čo dokážu reálne odsúhlasiť a zabezpečiť. Vojenské spôsobilosti v EÚ boli v posledných rokoch negatívne ovplyvnené nedostatočnými investíciami a znižovaním vnútroštátnych rozpočtov na obranu a vyznačujú sa vysokou mierou duplicity a fragmentácie. Okolnosti zhoršuje nedostatok spoločných technických noriem, čo je na úkor interoperability rôznorodých ozbrojených síl v Európe. Celkovo súčasné vojenské spôsobilosti členských štátov EÚ nezodpovedajú úrovni vojenských ambícií EÚ a ak by sa Európa mala brániť sama bez vonkajšej pomoci, na preklenutie tejto medzery by potrebovala niekoľko stoviek miliárd EUR. Odchod Spojeného kráľovstva Veľkej Británie a Severného Írska (ďalej len Spojené kráľovstvo) z EÚ túto situáciu ešte zhoršil, keďže výdavky Spojeného kráľovstva na obranu boli najvyššie v Európe a tvorili približne štvrtinu celkových výdavkov všetkých členských štátov EÚ na túto oblasť. (EDA, 2019)

Od roku 2017 vzniklo niekoľko iniciatív a mechanizmov súvisiacich s obranou, vrátane stálej štruktúrovanej spolupráce (z angl. Permanent Structured Cooperation - PESCO), koordinovaného výročného preskúmania v oblasti obrany (z angl. Coordinated Annual Review on Defence - CARD) a Európskeho obranného fondu (z angl. European Defence Agency - EDA). Tieto iniciatívy a navrhované zvýšenie financovania na úrovni EÚ a vnútroštátnych rozpočtov možno považovať za veľký krok vpred pre európsku obranu. Ich úspešnosť však vo veľkej miere závisí od niekoľkých kľúčových podmienok, ktoré sa v roku 2019 podľa audítorov nespĺňali. Ide predovšetkým o účinný proces plánovania v rámci EÚ, účasť členských štátov EÚ, vplyv na reálne potreby v oblasti spôsobilosti a rámec riadenia a zodpovednosti.

Vývoj na medzinárodnej scéne podnietil európskych lídrov, aby opätovne venovali pozornosť obrane ako kľúčovej politickej oblasti v súlade s narastajúcimi bezpečnostnými očakávaniami európskych občanov. Agresia zo strany RF, vývoj v oblasti transatlantických vzťahov, zintenzívnenie a diverzifikácia bezpečnostných hrozieb a obnovenie súperenia veľkých mocností priniesli v posledných rokoch nové podnety na obrannú spoluprácu v rámci Európskej Únie.

Európska komisia v marci 2019 iniciovala prvý spoločný projekt obranného priemyslu pod názvom Program rozvoja európskeho obranného priemyslu (z angl. European Defence Industrial Development Programme - EDIDP). Na výzvy na predkladanie návrhov v oblasti vývoja sa pridelil podiel z rozpočtu vo výške 500 mil. EUR, a to v týchto oblastiach:

1) umožnenie operácií, ochrany a udržateľnosti vojenských síl: 80 mil. EUR,
2) spravodajstvo, zabezpečená komunikácia a kybernetická obrana: 180 mil. EUR,
3) schopnosť vykonávať náročné operácie: 70 mil. EUR,
4) inovatívne obranné technológie (malé a stredné podniky): 27 mil. EUR.

Okrem toho Európska komisia vybrala dva projekty na priame pridelenie:

5) 100 mil. EUR na vývoj európskych dronov s dlhým doletom,
6) 37 mil. EUR na zabezpečený rádiový systém (európske zabezpečené softvérovo definované rádio).

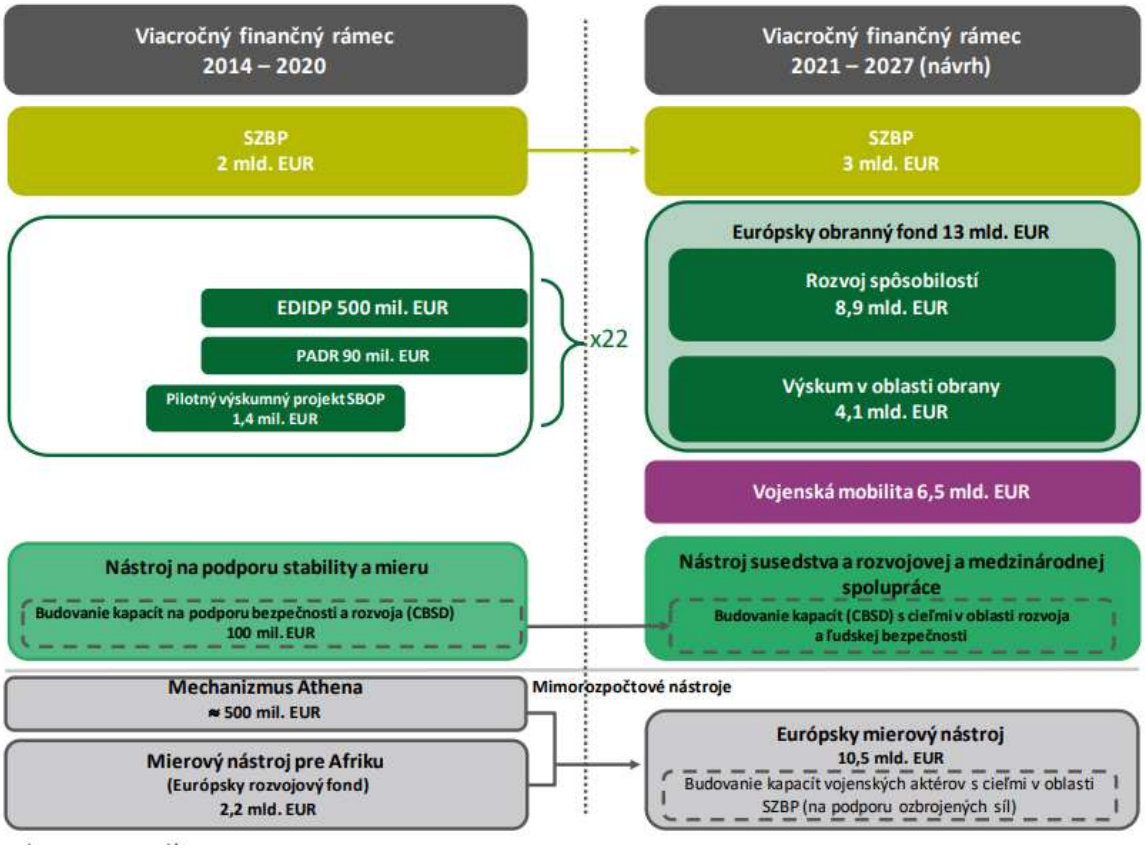
Druhým projektom v rámci Európskeho obranného fondu sa stala Prípravná akcia pre výskum v oblasti obrany (z angl. Preparatory Action on Defence Research - PADR): 90 mil. EUR. Na obdobie 2021 – 2027 Európska komisia navrhla zvýšiť výdavky na projekty výskumu a vývoja súvisiace s obranou z 590 mil. EUR na 13 mld. EUR, čím sa z 22 násobil rozpočet. (EDA, 2019)

Cieľom európskeho obranného fondu je pomáhať rozvoju konkurencieschopnosti, efektívnosti a inovačných kapacít európskeho obranného priemyslu. Zároveň tak má prispieť

k strategickej autonómnosti Únie. Na tieto účely sa fond zameriava na stimulovanie a podporu spoločných opatrení a cezhraničnej spolupráce prostredníctvom finančných stimulov pre právne subjekty v oblasti výskumu aj vývoja. Návrhy do budúcnosti Európskej komisie na viacročnom finančnom rámci 2021-2027 sa odráža ambícia, aby obrana zohrávala v budúcnosti dôležitejšiu úlohu. Obrázok 1. znázorňuje hlavné rozdiely medzi dvoma návrhmi rokov 2014-2020 a 2021-2027.

Európsky mierový nástroj, ktorého hodnota sa v období rokov 2021-2027 očakáva na úrovni 10,5 mld. EUR, stavia na existujúcich mechanizmoch. Spája ich do jedného fondu s cieľom preklenúť existujúce medzery a obmedzenia a posilniť schopnosť EÚ chrániť mier, predchádzať konfliktom a posilňovať medzinárodnú bezpečnosť. Návrh je zameraný na tri hlavné oblasti:

1) uľahčenie vojenských operácií EÚ zabezpečením trvalých finančných prostriedkov s rozšíreným rozsahom spoločných výdavkov v porovnaní s mechanizmom Athena[1],
2) rozšírenie rozsahu financovania operácií na podporu mieru z EÚ na tretie štáty a medzinárodné organizácie v globálnom meradle,
3) rozšírenie podpory EÚ na činnosti budovania spôsobilostí ozbrojených síl v partnerských krajinách.



Obrázok 1 Navrhované zmeny vo financovaní obrany EÚ
Zdroj: (EDA, 2019)

[1] Athena je mechanizmus, prostredníctvom ktorého sa spravuje financovanie spoločných nákladov súvisiacich s vojenskými operáciami EÚ v rámci spoločnej bezpečnostnej a obrannej politiky EÚ. Z mechanizmu Athena sa momentálne financuje 6 aktívnych vojenských operácií EÚ: EUFOR ALTHEA (Bosna a Hercegovina), EUNAVFOR ATALANTA (Africký roh), EUTM SOMALIA, EUTM MALI, EUTM RCA a EUNAVFOR MED IRINI. (Európska rada, 2019)

V tejto súvislosti Európska komisia navrhla značné zvýšenie rozpočtu EÚ na obranu a vonkajšiu bezpečnosť 22,5 mld. EUR na roky 2021-2027 v porovnaní s 2,8 mld. EUR v období 2014-2020. (EDA, 2019)

3 STRATEGICKÝ KOMPAS AKO AMBÍCIA PRE BEZPEČNOSŤ A OBRANU EURÓPSKEJ ÚNIE

21. marca 2022 bol prijatý dlho očakávaný Strategický kompas pre bezpečnosť a obranu (ďalej len Strategický kompas). Ten bol prijatý v čase, keď sme svedkami návratu vojny v Európe. Strategický kompas určuje do popredia EÚ jednotnejšiu ako kedykoľvek predtým. V dôsledku vojenskej intervencie RF voči Ukrajine, ktorá hrubo porušuje medzinárodné právo, zásady Charty OSN, oslabuje európsku a globálnu bezpečnosť a stabilitu. Ďalej vymedzuje EÚ odhodlanú brániť európsky bezpečnostný poriadok. Zvrchovanosť, územná celistvosť a nezávislosť v rámci medzinárodne uznaných hraníc by sa mali plne rešpektovať. Tým, že EÚ podporuje Ukrajinu preukazuje spolu s jej partnermi bezprecedentné odhodlanie obnoviť mier v Európe. Silnejšia a spôsobilejšia EÚ v oblasti bezpečnosti a obrany pozitívne prispeje ku globálnej a transatlantickej bezpečnosti a bude dopĺňať NATO, ktoré zostáva základom kolektívnej obrany jeho členov.

Agresívnejšie bezpečnostné prostredie si vyžaduje, aby EÚ učinila obrovský krok vpred a zvýšila vlastnú schopnosť a ochotu konať. EÚ musí posilniť svoju odolnosť aby zabezpečila solidaritu a vzájomnú pomoc. Solidarita medzi členskými štátmi sa odráža v článku 42 ods. 7 Zmluvy o Európskej Únii. V prípade, že sa členský štát stane na svojom území obeťou ozbrojenej agresie, ostatné členské štáty sú povinné mu poskytnúť pomoc a podporu všetkými dostupnými prostriedkami, v súlade s článkom 51 Charty Organizácie Spojených národov. Tým nie je dotknutá osobitná povaha bezpečnostnej a obrannej politiky niektorých členských štátov. (ZEÚ, 2012)

Ozbrojená agresia RF voči Ukrajine svedčí o pripravenosti použiť najvyššiu úroveň vojenskej sily. Bez akéhokoľvek ohľadu na právne alebo humanitárne aspekty. Kombináciu vytvára s hybridnými taktikami a kybernetickými útokmi. Modeluje zahraničnú manipuláciu s informáciami a dezinformáciami. Vytvára ekonomický a energetický nátlak a agresívnu rétoriku v jadrovej oblasti. RF sa takto aktívne snaží vytvoriť tzv. sféry vplyvu. Tieto agresívne a revizionistické činy, za ktoré je RF spolu s Bieloruskom plne zodpovedná, vážne a priamo ohrozujú európsky bezpečnostný poriadok a bezpečnosť európskych občanov. Osoby zodpovedné za tieto zločiny vrátane útokov na civilné obyvateľstvo a civilné objekty budú musieť byť brané na zodpovednosť.

Strategické partnerstvo EÚ s NATO má zásadný význam pre euroatlantickú bezpečnosť, ako sa opäť preukázalo v súvislosti s vojenskou agresiou RF voči Ukrajine v roku 2022. EÚ je naďalej plne odhodlaná ďalej posilňovať toto kľúčové partnerstvo, a to aj s cieľom podporiť transatlantické väzby. Na základe bezprecedentného pokroku, ktorý sa od roku 2016 dosiahol pri posilňovaní spolupráce s NATO, je potrebné podniknúť ďalšie ambiciózne a konkrétne kroky na vypracovanie spoločných odpovedí na existujúce a nové hrozby a spoločné výzvy. V rámci týchto spoločných vyhlásení a na základe zásad inkluzívnosti, reciprocity, otvorenosti a transparentnosti, ako aj autonómie rozhodovania oboch organizácií bude EÚ pokračovať v úzkej a vzájomne prospešnej spolupráci. EÚ bude ďalej posilňovať prebiehajúcu spoluprácu zameranú na politický dialóg, výmenu informácií, operácie krízového riadenia, rozvoj vojenských spôsobilostí a vojenskú mobilitu. Prehĺbenie EÚ bude vytvárať prostredníctvom spoločnej práce v oblasti posilnenia námornej bezpečnosti a boja proti hybridným hrozbám vrátane zabezpečenia kybernetického priestoru. Pre napĺňanie kompletného programu sa bude zameriavať na práva žien, mier a bezpečnosť. Okrem toho EÚ rozšíri spoluprácu v oblasti obrany, odolnosti, vznikajúcich a prelomových technológií a kozmického priestoru.

Strategický kompas predstavuje vysokú úroveň ambícií programu EÚ v oblasti bezpečnosti a obrany. EÚ sa zaväzuje poskytnúť spoločné posúdenie európskeho strategického prostredia, hrozieb a výziev, ktorým čelí. Prináša väčšiu súdržnosť a spoločnú víziu pre už prebiehajúce činnosti v oblasti bezpečnosti a obrany. Stanovuje nové spôsoby a prostriedky na zlepšenie kolektívnej schopnosti brániť a chrániť bezpečnosť občanov Únie. Určuje jasné ciele a míľniky na meranie dosiahnutého pokroku. Na tento účel sa zaväzuje vykonávať aktivity vždy, keď vypukne kríza a bude musieť byť schopná konať rýchlo a rázne, s partnermi, ak je to možné, a samostatne, ak je to potrebné. Na tento účel vytvorí kapacitu rýchleho nasadenia EÚ, ktorá umožní rýchlo nasadiť až 5 000 vojakov v obmedzujúcich prostrediach v rámci rôznych typov kríz. Posilní štruktúry velenia a riadenia EÚ a to najmä útvar pre plánovanie a vedenie vojenských operácií. Zvýši vlastnú pripravenosť a spoluprácu prostredníctvom zvýšenia vojenskej mobility a pravidelných taktických cvičení, zameraných najmä na kapacitu rýchleho nasadenia.

V rámci bezpečnosti sa EÚ zaväzuje posilniť schopnosť predvídať hrozby a zaručiť bezpečný prístup ku strategickým doménam. Posilní vlastné spravodajské kapacity, ako je rámec jednotnej kapacity EÚ na analýzu spravodajských informácií (z angl. Single Intelligence Analysis Capacity - SIAC) s cieľom zlepšiť Európske situačné povedomie a strategický výhľad. Vytvorí súbor hybridných nástrojov EÚ, ktorý by spájal rôzne nástroje umožňujúce odhaliť širokú škálu hybridných hrozieb a reagovať na ne. V tejto súvislosti vypracuje špecializovaný súbor nástrojov na riešenie manipulácie s informáciami a zasahovania zo zahraničia. Posilní vlastné činnosti v podzemnej, námornej, vzdušnej a kozmickej doméne. Rozšíri najmä koordinovanú námornú prítomnosť na ďalšie oblasti, počnúc čiernomorským teritóriom, a vypracuje stratégie pre bezpečnosť a obranu EÚ v oblasti kozmického priestoru. (Rada Európskej únie, 2022)

EÚ v reakcii na žiadosť Ukrajiny aktivoval svoju kybernetickú jednotku rýchlej reakcie (z angl. Cyber Rapid Response Team - CRRT), ktorá má pomôcť Ukrajine čeliť ruským kyberútokom. 22. februára 2022 dva dni pred inváziou RF na Ukrajinu to oznámil námestník litovského ministra obrany Margiris Abukevicius. Litva, ktorá tejto jednotke predsedá, a jeho ostatní členovia, aktivujú kybernetickú jednotku rýchlej reakcie, aby pomohli ukrajinským inštitúciám vysporiadať sa s rastúcou hrozbou kybernetických útokov. Kyberjednotka patrí medzi 60 bezpečnostných projektov PESCO. (Yar, 2022). Na základe týchto udalostí a žiadosti bude EÚ ďalej rozvíjať politický rámec EÚ pre kybernetickú obranu s cieľom lepšie sa pripraviť a reagovať na kybernetické útoky. Kybernetická obrana (priestor) bude plne previazaná s podzemnou, vzdušnou, námornou a kozmickou doménou.

Ambície a opatrenia, ktoré sme vyjadrili sú zároveň opísané v Strategickom kompase sú ambiciózne, ale možno ich dosiahnuť trvalým politickým úsilím. Strategický kompas poskytuje strategickú perspektívu a podrobne opisuje nástroje a iniciatívy potrebné na zabezpečenie rýchlejšej, rozhodnejšej a náznejšej činnosti EÚ. Napriek významnému pokroku dosiahnutému v posledných rokoch je EÚ ako celok nedostatočne vybavená na boj proti širokému spektru hrozieb a výziev, ktorým čelí. Vzhľadom na súčasné bezpečnostné výzvy je nevyhnutné vykonať rýchle zmeny a zmenšiť priepasť medzi ambíciami a skutkami Európskej Únie.

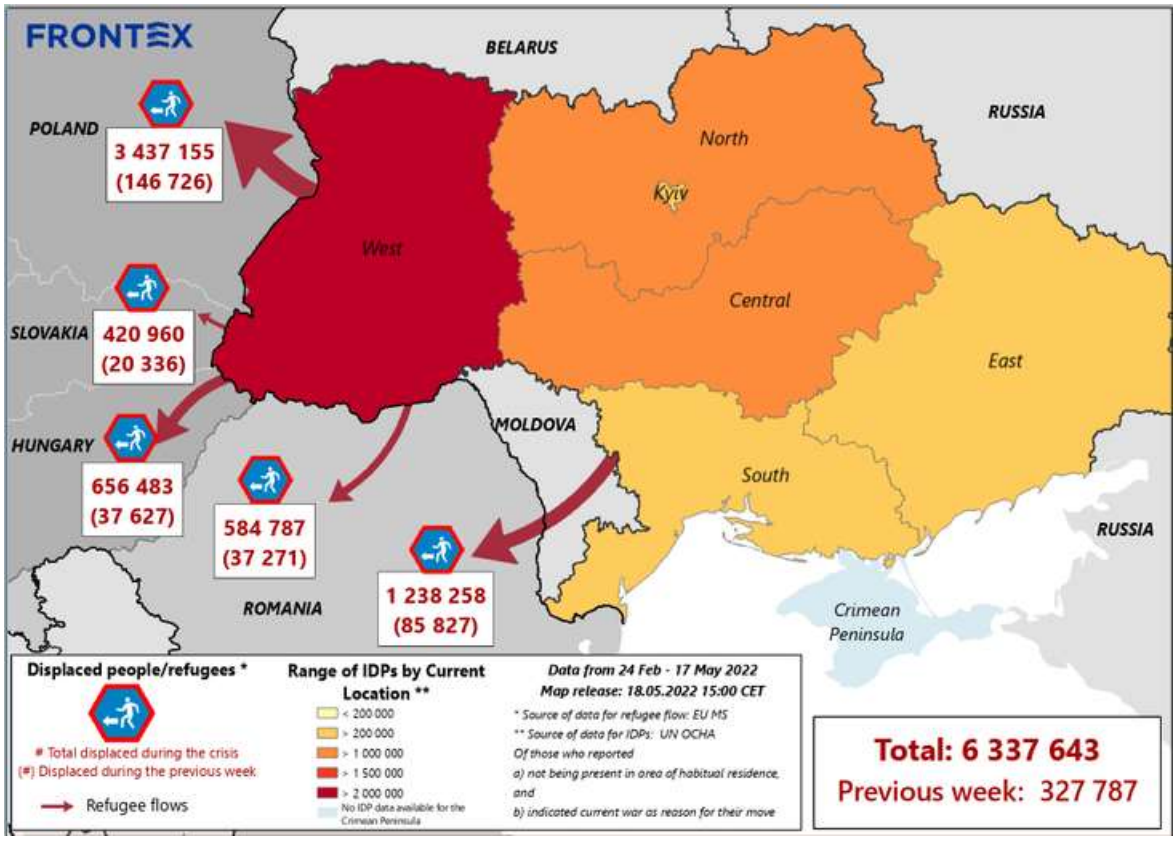
4 MEDZINÁRODNÁ POMOC, MIGRÁCIA A DOČASNÁ OCHRANA UKRAJINSKÝCH OBČANOV V EURÓPSKEJ ÚNII

V decembri 2014 bola na Ukrajinu vyslaná Európska poradná misia EUAM (z angl. The European Union Advisory Mission Ukraine). Táto misia koordinuje medzinárodnú pomoc v oblasti civilnej bezpečnosti a okrem bežnej operatívnej činnosti poskytuje ukrajinským

orgánom strategické poradenstvo. Súčasťou je aj školenie v otázkach budovania udržateľných, verejne zodpovedných a účinných bezpečnostných služieb posilňujúcich právny štát.

Odkedy sa začala útočná invázia RF proti Ukrajine v roku 2022, misia EUAM už nie je schopná plne vykonávať svoj mandát na území Ukrajiny. EÚ však naďalej stojí pri svojich ukrajinských partneroch a podporuje ich v oblasti reformy civilného bezpečnostného sektora a na ceste k Európskemu spoločnému cieľu vidieť Ukrajinu ako nezávislý a prosperujúci štát s obyvateľmi, ktorí žijú slobodne, v mieri, dodržujú ľudské práva a uznávajú právny štát. V marci a apríli 2022 členské štáty EÚ zadali misii EUAM nové úlohy. Misia teraz poskytuje podporu orgánom presadzovania práva s cieľom uľahčiť pohyb utečencov z Ukrajiny do susedných členských štátov a vynaložiť úsilie humanitárnej pomoci na Ukrajinu. EUAM tiež podporuje inštitúcie právneho štátu s cieľom uľahčiť vyšetrovanie a stíhanie medzinárodných zločinov. (EUAM, 2022)

Európska únia je priamo ovplyvnená konfliktom na Ukrajine na svojich východných hraniciach. Od začiatku agresie RF na Ukrajine narastá migračný tlak. Obyvatelia Ukrajiny hľadajú ochranu v členských štátoch EÚ. Do EÚ cez Poľsko, Slovensko, Maďarsko a Rumunsko prešlo legálne od 24. februára 2022 do 17. mája 2022 viac ako 6 337 643 vysídlených osôb. Pri rastúcom napätí sa očakáva zvýšenie týchto počtov. EÚ preukázala podporu občanom Ukrajiny, ktorí čelia bezprecedentnému aktu agresie zo strany RF. Na tento akt zareagovalo aj OSN a vyhlásilo naliehavú humanitárnu výzvu v súvislosti s potrebami ochrany a pomoci na Ukrajine. OSN vypracovalo regionálny plán pre utečencov z Ukrajiny, v ktorom sa uvádzajú podrobné údaje o počtoch ľudí v núdzi a tých, na ktorých sa má pomoc zamerať. Cieľom týchto krokov bola reakcia na túto situáciu a stanovila sa skutočnosť, že došlo k hromadnému prílevu vysídlených osôb a zaviedla sa dočasná ochrana dotknutých vysídlených osôb. (Frontex, 2022)



Obrázok 2 Migračná vlna
Zdroj: (Frontex, 2022)

Dočasná ochrana je v súčasnej situácii najvhodnejším nástrojom. Vzhľadom na mimoriadnu a výnimočnú povahu vojenskej inváze RF na Ukrajinu a rozsah hromadného prílevu by dočasná ochrana mala umožniť vysídleným osobám používať v celej Únii harmonizované práva, ktoré poskytujú primeranú úroveň ochrany. Zo zavedenia dočasnej ochrany by mali prospech aj členské štáty EÚ, keďže práva spojené s dočasnou ochranou obmedzujú potrebu vysídlených osôb okamžite žiadať o medzinárodnú ochranu, a tak aj riziko preťaženia azylových systémov členských štátov, keďže znižujú formality na minimum z dôvodu naliehavosti situácie.

Keďže Ukrajina splnila kritériá akčného plánu liberalizácie vízového režimu, začal sa pre ukrajinských občanov s biometrickým pasom od 11. júna 2017 uplatňovať bezvízový styk[2] pre vstup do EÚ. Držitelia ukrajinských biometrických pasov sú preto pri cestovaní do EÚ oslobodení od vízovej povinnosti. Na základe skúseností po protiprávnej anexii Krymskej autonómnej republiky a mesta Sevastopoľ zo strany RF a po vojne na východnej Ukrajine sa očakáva, že polovica ukrajinských utečencov prichádzajúcich do EÚ, ktorí využívajú bezvízový styk, sa pripojí k rodinným príslušníkom alebo si bude hľadať zamestnanie v EÚ. Zatiaľ čo druhá polovica môže požiadať o medzinárodnú ochranu. V praxi to uľahčí rozloženie úsilia medzi členskými štátmi, čím sa zníži tlak na vnútroštátne prijímacie systémy.

V Smernici 2001/55/ES z 20. júla 2001 o minimálnych štandardoch na poskytovanie dočasnej ochrany v prípade hromadného prílevu vysídlených osôb a o opatreniach na podporu rovnováhy úsilia medzi členskými štátmi pri prijímaní takýchto osôb a znášaní z toho vyplývajúcich dôsledkov. Vyplýva náležitosť zohľadňujúce povinnosti členských štátov EÚ, pokiaľ ide o udržiavanie verejného poriadku a zabezpečovanie vnútornej bezpečnosti. Smernica umožňuje členským štátom vylúčiť vysídlenú osobu z dočasnej ochrany, ak existujú vážne dôvody domnievať sa, že daná osoba spáchala zločin proti mieru, vojnový zločin alebo zločin proti ľudskosti. Medzinárodné prostriedky si kladú za cieľ vydanie opatrení vo vzťahu k takýmto trestným činom. Spáchanie závažných trestných činov nepolitického charakteru mimo prijímajúceho členského štátu pred tým, ako bola prijatá osoba do tohto členského štátu ako osoba požívajúca dočasnú ochranu, alebo ide o osobu, ktorá je vinná z konania v rozpore s cieľmi a zásadami OSN. Smernica takisto umožňuje členským štátom vylúčiť vysídlenú osobu z dočasnej ochrany. Ak existujú opodstatnené dôvody na to, aby bola považovaná za osobu ohrozujúcu bezpečnosť hostiteľského členského štátu alebo predstavujúcu nebezpečenstvo pre spoločnosť hostiteľského štátu. (Carmona, Csaszi, 2021)

5 EURÓPSKA BEZPEČNOSŤ V SUBORDINÁCII SEVEROATLANTICKEJ ALIANCII

V kontexte útoku RF na Ukrajinu, švédska vláda 16. marca 2022 rozhodla zriadiť pracovnú skupinu na zhodnotenie zmien v bezpečnostnom prostredí po tejto agresii. Pracovná skupina vypracovala dokument Zhoršenie bezpečnostného prostredia – dôsledky pre Švédsko (z angl. Deterioration of the security environment – implications for Sweden), ktorý 13. mája 2022 verejne predstavila ministerka zahraničných vecí Ann Lindeová.

Správa neobsahuje žiadne konkrétne odporúčania ale jej záverom je, že členstvo v NATO bude mať stabilizačný účinok a bude prínosom pre krajiny okolo Baltského mora. V konečnom dôsledku navrhuje ukončenie viac ako 200 rokov švédskej neangažovanosti. Podľa správy je členstvo v NATO pre Švédsko výhodnejšie, fungovalo by ako odstrašujúci

[2] Nariadenie (EÚ) 2018/1806, v ktorom sa uvádza zoznam tretích krajín, ktorých štátni príslušníci musia mať víza pri prekračovaní vonkajších hraníc členských štátov EÚ a krajín, ktorých štátni príslušníci sú oslobodení od tejto povinnosti, pokiaľ ide o pobyty, ktorých dĺžka nepresahuje 90 dní v rámci akéhokoľvek 180 dňového obdobia. Oslobodenie od vízovej povinnosti sa vzťahuje len na držiteľov biometrických pasov vydaných Ukrajinou v súlade s normami Medzinárodnej organizácie civilného letectva.

prostriedok a zvýšilo bezpečnosť krajiny. Správa taktiež uvádza, že nie je realistické rozvíjať bilaterálne obranné aliancie mimo existujúcich európskych a euroatlantických štruktúr. (GOSW, 2022)

V dôsledku na vzniknuté udalosti reagovala rovnako aj fínska vláda, ktorá zverejnila 13. apríla 2022 správu o zmenách v bezpečnostnom prostredí (z angl. Government report on changes in the security environment). Dokument bol vypracovaný ako reakcia na zásadné zmeny v bezpečnostnom prostredí, ktoré nastali po invázii RF na Ukrajinu. Správa hodnotí zmeny v operačnom a bezpečnostnom prostredí a vplyvy zmenenej bezpečnostnej situácie na ekonomiku, odolnosť, bezpečnosť dodávok, vnútornú bezpečnosť, kybernetickú bezpečnosť, hybridné a vplyvové aktivity a kritickú infraštruktúru.

Správa sa zaoberá rozvojom obranyschopnosti krajiny, EÚ ako aktérom bezpečnostnej politiky a užšou bilaterálnou spoluprácou so Švédskom, Nórskom, ďalšími severskými krajinami, USA a Spojeným kráľovstvom a iniciatívami multilaterálnej obrannej spolupráce. Hodnotí sa aj užšia spolupráca s NATO a dopady prípadného členstva Fínska v NATO. Podľa záverov správy ak by sa Fínsko pripojilo k NATO, odstrašujúci účinok by bol značne silnejší, než je v súčasnosti, keďže by bol založený na schopnostiach celej Aliancie. Správa pojednáva, že v reakcii na zmenenú bezpečnostnú situáciu bude Fínsko pokračovať v aktívnej a proaktívnej diplomacii, posilňovať svoju obranyschopnosť a zintenzívňovať spoluprácu s kľúčovými partnermi. Zdôrazňuje sa dôležitosť zachovania odolnosti spoločnosti, národnej obrany a vnútornej bezpečnosti pre bezpečnosť Fínska. Správa je východiskovým dokumentom k debate o prípadné členstvo Fínska v Aliancii. (FG, 2022)

Na základe aj týchto vypracovaných dokumentov Švédsko a Fínsko 17. mája 2022 požiadalo o vstup do NATO. Vstup týchto dvoch krajín do NATO zamýšľalo zablokovať Turecko. Turecký prezident Erdogan označil obe krajiny za útočisko pre teroristické organizácie. Príčinou sporu je azyl, ktorý poskytli prenasledovaným predstaviteľom kurdských organizácií, ktoré Turecko označuje za teroristické. Predstavitelia NATO a iných členských krajín však boli presvedčený, že Turecko nebude rozšírenie vetovať. Kanadská ministerka zahraničných vecí Mélanie Joly na rokovaní v Bruseli vyhlásila, že prioritou je čo najviac skrátiť prístupový proces. Ak budú severské krajiny úspešné, členom NATO už nebudú len štyri krajiny EÚ: Cyprus, Írsko, Malta a Rakúsko. Rakúsky minister zahraničných vecí už oznámil, že jeho krajina sa do NATO nechystá. Argumentoval aj inou geografickou polohou než Fínsko a Švédsko, ktoré majú s RF spoločné suchozemské, resp. námorné hranice. Zástupca ministra obrany RF Sergej Riabkov pre agentúru Ria Novosti vyhlásil, že týmto krokom sa bezpečnosť Fínska a Švédska nezvýši, pretože narastie politické a vojenské napätie. (Geist - Euractiv, 2022)

Po ruskej anexii Krymu členské štáty na summite NATO vo Walese v septembri roku 2014 schválili tzv. Akčný plán pripravenosti (z angl. Readiness Action Plan - RAP). Cieľom bolo posilniť kolektívnu obranu Aliancie, odstrašiť všetkých potenciálnych nepriateľov a ubezpečiť štáty na východnej hranici Aliancie o záväzkoch NATO v súvislosti s článkom 5 Washingtonskej zmluvy. V dôsledku zhoršenia bezpečnostnej situácie v Európe po útoku RF na Ukrajinu spojenci rozhodli o posilnení východného krídla NATO rozšírením predsunutej prítomnosti NATO do štyroch ďalších krajín na Slovensko, do Maďarska, Rumunska a Bulharska.

Poslať vojenské jednotky na Ukrajinu a zapojiť sa tak do vojny na Ukrajine NATO neplánuje, ale objektívne ani nemôže. Aj napriek tomu je však jasné, že sa členské krajiny NATO nemôžu len tak prizerať. Na obdobie dlhotrvajúceho napätia s agresívnou a nepredpokladateľnou víziou RF je potrebné sa pripraviť a preto NATO pristúpilo k posilneniu tzv. východného krídla Aliancie.

Ochrana východného krídla NATO bude posilnená o:

- 40 000 vojakov pod priamym velením NATO,
- viac ako 200 000 vojakov pod národným velením štátov východného krídla NATO,
- 100 000 amerických vojakov v celej Európe,
- 130 stíhacích lietadiel, ktoré budú monitorovať vzdušný priestor 24 hodín a 7 dní v týždni,
- 140 spojeneckých lodí,
- postupné obsadzovanie obranných bojových skupín na Slovensku, v Maďarsku, Bulharsku a Rumunsku,
- nasadenie systémov protivzdušnej obrany (Patriot) na Slovensku.

Obranné a odstrašujúce posilnenie východného krídla presadzuje aj Slovensko. Vláda a parlament pôsobenie aliančných vojakov na našom území schválili. Pôjde o maximálne 2100 vojakov, z ktorých by malo byť 600 z Českej republiky. (Hrozenská, 2022)

Obrázok 3 Východné krídlo NATO - Jún 2022
Zdroj: (NATO, 2022)

V súvislosti so vzniknutou situáciou na Ukrajine je obnovený záväzok NATO zamerať sa prioritne na kolektívnu bezpečnosť, ako aj záväzok vo vzťahu k článku 5 Washingtonskej zmluvy. Rozhodnutia prijaté na samite NATO v Newporte týkajúce sa zvýšenia úrovne bezpečnosti spojencov vo východnej Európe vrátane vytvorenia jednotky rýchleho nasadenia, stálej rotujúcej vojenskej prítomnosti NATO a vytvorenia logistickej infraštruktúry. Ako aj úsilia zameraného na posilnenie schopnosti Ukrajiny chrániť svoju vlastnú bezpečnosť. Berie na vedomie, že spojenci NATO môžu na bilaterálnej úrovni poskytnúť Ukrajine potrebné zbrane, technológie a odborné znalosti v záujme ich bezpečnosti a obrany, rozhodne však zdôrazňuje, že neexistuje momentálne žiadne vojenské riešenie ukrajinskej krízy. (Európska rada, 2022)

ZÁVER

Zasahovanie RF do politického vývoja, smerovanie Ukrajiny do EÚ a najmä anexie Krymu v roku 2014 vyvolali celosvetovú pozornosť. Sú všeobecne hodnotené ako prejav ruskej expanzívnosti a agresivity. Členské štáty EÚ jednotne odsúdili súčasnú ruskú agresiu. Mier, bezpečnosť a stabilita v Európe už nie sú samozrejmosťou. Z našich dostupných informácií vyvodzujeme tvrdenie, že západné a najmä európske krajiny začali po udalostiach na Ukrajine v roku 2014 vnímať RF ako agresora, ktorý svojím konaním porušuje normy medzinárodného práva. Priama i nepriama vojenská intervencia RF na Ukrajine predstavuje porušenie medzinárodného práva a obzvlášť aj záväzkov RF vyplývajúce z Charty OSN. Pripomíname predovšetkým článok 2 Charty OSN, ktorý členské štáty vyzýva, aby sa vo svojich vzájomných vzťahoch zdržali sily alebo hrozby silou, a vyzvalo členské štáty, aby agresiu zo strany RF odsúdili. Zároveň RF naďalej odmieta vykonávať Zmluvu o konvenčných ozbrojených silách v Európe, ktorá je jedna zo základných pilierov európskej bezpečnosti. Zároveň aj NATO na svojom summite vo Walese v roku 2014 anexiu Krymu odsúdilo ako porušenie medzinárodného mieru, ako pohŕdanie medzinárodným právom a vážnu výzvu pre bezpečnosť celej euroatlantickej oblasti a vyzvala RF na stiahnutie všetkých vojsk z územia Krymu. Dôsledkom tejto pozície voči RF bolo prijatie rozsiahlych sankcií a ochladenie diplomatických vzťahov.

Môžeme konštatovať, že NATO a jej princíp kolektívnej obrany, najmä z pohľadu na článok 5 zmluvy o Severoatlantickej aliancii je nespochybniteľný ručiteľ Európskej bezpečnosti. Odhliadnuc od toho, že EÚ aj NATO sú medzivládne organizácie, NATO bolo primárne sformované pre zaručenie bezpečnosti na rozdiel od EÚ, ktorá bola založená ako ekonomická únia, doteraz postrádajúca vlastnú štruktúru obrany a bezpečnosti. Faktom je, že NATO ani EÚ nemajú vlastné ozbrojené sily, a teda vyžadujú určitú bojaschopnosť od členských štátov. Hlavný rozdiel v prospech NATO je však ten, že má vlastné štandardy, praktiky, inštitúcie a koordináciu. Tieto atribúty mu dávajú väčšiu dominanciu ako EÚ. Bližší pohľad na členské štáty EÚ jasne ukazuje, že až na pár výnimiek nie sú až tak ochotné plniť si svoje záväzky voči NATO, predovšetkým pokiaľ ide o výdavky na obranu.

Vstup Ukrajiny do EÚ poskytuje bezpečnosť v súlade s článkom 42 Zmluvy o Európskej únii. Ak by sa teda Ukrajina stala členom EÚ, tá by sa zaviazala podniknúť všetky potrebné kroky na obranu Ukrajiny pred nevyprovokovanou agresiou RF. To by mohlo aktivovať obranný pakt EÚ, čo by výrazne zvýšilo riziko vojny medzi NATO a RF, pretože 21 členských štátov EÚ je aj súčasťou NATO. Aby tomu zabránila, EÚ by musela vylúčiť Ukrajinu z obranného paktu.

Zvýšením výdavkov na obranu a zabezpečením prítomnosti vojenských síl organizácie NATO sa aspoň čiastočne vytvára pocit bezpečia pre obyvateľov členských štátov EÚ. Môžeme očakávať, že zvyšovanie výdavkov na obranu je len prvým krokom k vytvoreniu stabilného a bezpečného prostredia, ktoré by bolo schopné čeliť súčasnému a potenciálnemu budúcemu tlaku RF. Na strane druhej je potrebné tieto krajiny podporiť nielen vojensky, ale aj ekonomicky. Dôraz sa kladie na ich snahy diverzifikovať hospodárstvo a zbaviť sa ekonomickej závislosti od Ruskej federácie.

Pokiaľ bude RF naďalej narúšať hranice stanovené medzinárodným právom a svojou agresívnou politikou šíriť svoj vplyv, tak nebude a nemôže byť vnímané zo strany EÚ ako spoľahlivý partner. EÚ v súčasnosti vníma RF ako nevyspytateľného agresora, ktorý porušením medzinárodného práva anektoval územie iného štátu, a na strane druhej je ako nutné zlo pri riešení niektorých otázok medzinárodnej spolupráce. Takýto postoj EÚ bude podľa nášho názoru pretrvávať dovtedy, kým ruský režim nebude konať v súlade s medzinárodným právom.

V rámci budúceho vývoja bezpečnostnej situácie je naliehavo potrebné posilniť obranyschopnosť Ukrajiny, o čo žiadajú ukrajinské orgány. EÚ by mala preskúmať spôsoby,

ako pomôcť ukrajinskej vláde pri posilňovaní jej obranných schopností. EÚ by mala pracovať na komunikačnej stratégii s cieľom bojovať proti propagandistickej kampani RF, ktorá je namierená proti Európe, Ukrajine a v podstate samotnej RF. Ukrajina môže riadne fungovať len vtedy, ak bude existovať efektívne presadzovanie práva, vojenské spravodajstvo a obranný sektor.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

CARMONA, F. – CSASZI, L. 2021. *Informačné listy o Európskej Únii*. Tri susedné krajiny Východného partnerstva: Ukrajina, Moldavsko a Bielorusko. Európsky parlament. November 2021. [online]. Dostupné na: https://www.europarl.europa.eu/factsheets/sk/sheet/171/tri-susedne-krajiny-vychodneho-partnerstva-ukrajina-moldavsko-a-bielorusko

GEIST, R. - Euractiv, 2022. *Švédsko požiada o vstup do NATO, Fíni to už urobili*. [online]. Dostupné na: https://euractiv.sk/section/zahranicie-a-bezpecnost/news/svedsko-poziada-o-vstup-do-nato-fini-to-uz-urobili/

HROZENSKÁ, B. 2022. *Predsunutá prítomnosť NATO na východnej hranici sa posilňuje*. Analytický útvar Ministerstvo obrany SR, článok č. 3-2022, 2.s. Bratislava. [online]. Dostupné na: https://www.mosr.sk/data/files/4734_2022-c-03-predsunuta-pritomnost-nato-na-vychodnej-hranici-sa-posilnuje.pdf

HUNTINGTON, S.P. 2001. *Stret Civilizácií, Boj kultúr a premena svetového poriadku*. Praha. Rybka Publisher. 2001, s 27. ISBN 80-86182-49-5

YAR, L. 2022. *Únia na Ukrajine po prvýkrát nasadí sily, ktoré vznikli ako jeden z jej obranných projektov*. [online]. Dostupné na: https://euractiv.sk/section/obrana-a-zahranicie/news/unia-na-ukrajine-po-prvy-krat-nasadi-sily-ktore-vznikli-ako-jeden-z-jej-obrannych-projektov/

EDA. 2019. *Preskúmanie EDA č. 9/2019 Európska obrana*. Európska obranná agentúra - Európsky dvor audítorov. ECA Press Luxemburg. [online]. Dostupné na: https://www.eca.europa.eu/sk/Pages/DocItem.aspx?did={A75B26BC-F737-4C55-A615-A4E37055E5EC}

Európska rada. 2019. *Athena – financovanie bezpečnostných a obranných vojenských operácií*. [online]. Dostupné na: https://www.consilium.europa.eu/sk/policies/athena/

Európska rada. 2022. *Reakcia EÚ na inváziu Ruska na Ukrajinu*. [online]. Dostupné na: https://www.consilium.europa.eu/sk/policies/eu-response-ukraine-invasion/

EUAM. 2022. EUAM Ukraine about us. [online]. Dostupné na: https://www.euam-ukraine.eu/our-mission/about-us/

Frontex. 2022. *Update on Ukraine: more than 6 million refugees cross EU's borders*. [online]. Dostupné na: https://frontex.europa.eu/media-centre/news/news-release/update-on-ukraine-6-3-million-refugees-enter-the-eu-from-ukraine-and-moldova-GTZbZs

FG. 2022. *Government report on changes in the security environment*. Finnish Government, Ministry for Foreign Affairs of Finland, Helsinki. 13.4.2022. 53.s. [online]. Dostupné na: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164002/VN_2022_20.pdf?sequence=4&isAllowed=y

GOSW. 2022. *Deterioration of the security environment – implications for Sweden*. Government offices of Sweden, Ministry for Foreign Affairs. 16.3.2022 51.s. [online]. Dostupné na: https://www.government.se/49acb4/contentassets/05ffb51ba6404a459d7ee45c98e87a83/deterioration-of-the-security-environment---inplications-for-sweden-ds-20228

NATO. 2022. *NATO's military presence in the east of the Alliance*. [online]. Dostupné na: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/2203-map-det-def-east.pdf

Smernica Rady 2001/55/ES z 20. júla 2001 o minimálnych štandardoch na poskytovanie dočasnej ochrany v prípade hromadného prílevu vysídlených osôb a o opatreniach na podporu rovnováhy úsilia medzi členskými štátmi pri prijímaní takýchto osôb a znášaní z toho vyplývajúcich dôsledkov. Úradný vestník Európskej únie. 2001. 10.s [online]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32001L0055&from=SK

SZBP. 2016. *Spoločná zahraničná a bezpečnostná politika – globálna stratégia*. Európska únia, Brusel 2016, 43.s. [online]. Dostupné na: http://mepoforum.sk/wp-content/uploads/2016/09/EU-globalna-strategia-sk.pdf

Rada Európskej únie. 2022. *Strategický kompas pre bezpečnosť a obranu*. Rada Európskej únie: Generálny sekretariát rady, 21. marca 2022, Brusel. 47.s. [online]. Dostupné na: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sk/pdf

ZEÚ. 2012. *Zmluva o Európskej únie* (konsolidované znenie). Úradný vestník Európskej únie. 26.10.2012. 34.s. [online]. Dostupné na: https://eurlex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506 fd71826e6da6.0011.02/DOC_1&format=PDF

kpt. Ing. Martin BAKIČ
Externý doktorand katedry bezpečnosti a obrany
Akadémia ozbrojených síl gen. M. R. Štefánika, Demänová 393, 031 01 Liptovský Mikuláš,
Email: mattibak@gmail.com

POSUDZOVANIE RIZIKA – IDENTIFIKÁCIA, ANALÝZA A HODNOTENIE RIZIKA

RISK ASSESSMENT - IDENTIFICATION, ANALYSIS AND EVALUATION

Lubomír BELAN, Ján MIŠÍK

ABSTRACT

The author's goal is to inform readers about the use of risk assessment, which is part of risk management. As part of this issue, it is determined how the goals of the organization can be affected due to their ongoing processes. A number of people deal with the issue of risk management and use it as an aid on the basis of which risks are identified, analysed and evaluated in terms of consequences and their probability.

Keywords: risk assessment, risk identification, risk analysis, risk evaluation

ÚVOD

Organizácia či objekt existujúci v neistom, stále sa meniacom prostredí, musí mať schopnosť prispôsobiť sa alebo zmeniť sa v záujme dosiahnutia určitého súladu vlastnej činnosti, vlastných cieľov s podmienkami okolia, ktoré sa menia a ktoré môžu byť zdrojom narušenia stability so všetkými svojimi vplyvmi na jednotlivé faktory širšieho a bezprostredného externého prostredia.

„Mnohopočetné informácie, správy a údaje o prírodných katastrofách, priemyselných haváriách, ozbrojených konfliktoch a incidentoch, teroristických a ozbrojených útokoch, organizovanom zločine a kriminalite, epidémiách a pandémiách a o mnohých ďalších negatívnych javoch a tragických udalostiach svedčia o tom, že ľudstvo nedodržiava alebo nedostatočne zdieľa hodnoty, požiadavky a zásady bezpečnosti“. (Ivančík, 2021, s.40) Človek (manažér, veliteľ), ako hlavný subjekt bezpečnosti, preto nevyhnutne potrebuje na plnenie svojich úloh v oblasti zaisťovania bezpečnosti mať poznatky, skúsenosti, metodické a iné nástroje. Inými slovami, potrebuje ovládať aj teóriu manažérstva rizík. (Ivančík, 2021)

Manažérstvo rizika je preto jedným z najdôležitejších problémov, ktorým dnes organizácie čelia. Je dôležitou súčasťou každého strategického riadenia organizácie. Predstavuje proces, prostredníctvom ktorého sa organizácie venujú rizikám spojeným s činnosťami organizácie, s cieľom dosiahnuť trvalý prospech z každej jednotlivej a súhrnne zo všetkých činností organizácie.

Posudzovanie rizík patrí medzi časť manažérstva rizika, ktorá poskytuje štruktúrovaný proces, pri ktorom sa zisťuje, ako môžu byť ovplyvnené ciele organizácie a pomocou ktorej sa analyzujú riziká v zmysle následkov a ich pravdepodobnosti predtým, než sa rozhodne, či je potrebné ďalšie zaobchádzanie s rizikom. (Belan, 2015) Posudzovanie rizika je súhrnný proces:

a) *identifikácie rizík* – proces, ktorý sa používa na nájdenie, preskúmanie a popísanie rizík, ktoré by mohli ovplyvniť dosiahnutie cieľov (zámerov),

b) *analýzy rizík* – proces, ktorý sa používa na pochopenie podstaty, zdrojov a príčin rizík na určenie a ocenenie úrovne rizika, používa sa aj na skúmanie ich dopadov a následkov a prieskum zavedených opatrení na riadenie rizika,
c) *hodnotenia rizík* – proces, ktorý sa používa na porovnanie výsledkov analýzy rizík s kritériami rizika a rozhodnutie či zistená úroveň rizika je prijateľná, neprijateľná alebo prípustná.

Návod na spôsoby posudzovania rizika poskytuje norma ISO/IEC 31010:2019 – Risk management – Risk Assessment Techniques, v SR prevzaté ako STN EN 31010:2021 (010380) Manažérstvo rizika – Techniky posudzovania rizika.

1 Proces posudzovania rizík

Vstup pre posudzovanie rizika tvorí určenie súvislostí a definovanie kritérií rizika. ***Výstup*** z posudzovania rizík je vstupom do procesov rozhodovania danej organizácie – zoznam rizík, ktoré vyžadujú zaobchádzanie. Spôsob, akým sa proces posudzovania rizík uskutoční, nezáleží iba na súvislostiach procesu manažérstva rizika, ale tiež na metódach použitých pri vykonávaní posudzovania rizík.

1.1 Identifikácia rizík

Identifikácia rizika zahŕňa identifikáciu:
- zdrojov rizika – prvkov, ktoré samy osebe alebo v kombinácii majú vnútorný potenciál vyvolať riziko a oblasti ich následkov,
- udalostí, ktoré zdroje rizika môžu spôsobiť,
- okolností, ktoré by mohli mať potenciálne následky na dosiahnutie cieľov,
- príčin rizika – toho, ***ČO*** sa môže stať, ***KEDY*** a ***KDE***, ***PREČO*** a ***AKO*** sa to môže stať,
- potenciálnych následkov**,**
- opatrení zavedených na modifikáciu rizika.

Cieľom identifikácie rizík je vytvoriť obsažný *zoznam rizík*, založený na udalostiach**,** ktoré by mohli ***vytvoriť, podporiť, zabrániť, znehodnotiť, urýchliť, alebo pozdržať dosiahnutie zámerov.*** (Belan, 2015)

Identifikácia rizík sa uskutočňuje na začiatku procesu (projektu, úloha a pod.) a počas celého jeho chodu. Riziká je nutné identifikovať včas. Je jedno aká metóda alebo forma sa použije na popísanie rizík, ale je potrebné dodržať ju v celej organizácii. „Efektívnosť procesu identifikácie rizika možno hodnotiť napr. počtom kladných odpovedí minimálne na tieto otázky: (Varcholová, Dubovická, 2008, str. 70)
- *Je zabezpečená identifikácia celého rozsahu rizík?*
- *Je zabezpečený nepretržitý proces mapovania rizika?*
- *Vyžíva sa mapovanie rizika dôsledne a efektívne?*
- *Sú výsledky riadenia rizík integrované do stratégií a plánov?“*

Výsledkom identifikácie rizík je ***zoznam rizík*** – tabuľka 1, ktorý slúži k zostaveniu registra rizík. Ten sa dosť často zapisuje ako tabuľka. Register rizík by mal obsahovať identifikačné číslo rizika, jeho meno (názov), popis, hodnotu rizika a dopady. (Belan, 2015)

Tabuľka 1 Možný obsah Zoznamu rizík

Číslo rizika	R1 – Rx
Názov rizika	Napr. Úmyselné napadnutie majetku
Popis rizika	Kvalitatívny popis udalostí, miesto, rozsah, druh, počet a závislosti, prostredie, úmysel, čo sa môže stať v budúcnosti a možný dopad na organizáciu, napr. *vlámanie do priestoru garáže, možnosť krádeže vozidiel, PHM, narušenie dopravnej kapacity organizácie a pod.*
Kategória rizika	Napr. strategické, prevádzkové, finančné, *bezpečnostné* a iné
Zodpovednosť za riziko, zainteresované strany	Vlastník rizika – fyzická osoba zodpovedná za zabezpečenie toho, že pracovníci sa zodpovedným spôsobom zoznámili s vykonávanými protiopatreniami Zainteresované strany, ich očakávanie a záujmy
Dátum hlásenia	Dátum, kedy bolo riziko prvýkrát zaznamenané (DD-MM-RR)
Posledná aktualizácia	(DD-MM-RR)
Pravdepodobnosť	Veľmi malá, malá, stredná, veľká, veľmi veľká
Následok	Veľmi malý, malý, stredný, veľký, veľmi veľký
Popis následku	Konkrétne dopady rizika – potenciál a veľkosť možných strát / ziskov, ohrozená hodnota, náklady na riziko, napr. možná krádež dvoch nákladných aut a 100 l nafty, veľká finančná strata, náklady na opravu
Časová os	Blízky termín, stredný termín, ďaleký termín, podľa definovania časovej osi
Opatrenia na modifikáciu rizika	Ako je riziko v súčasnosti riadené, spôsob monitorovania a kontroly Miera dôvery (spoľahlivosť) v súčasný spôsob riadenia rizika Určenie možných postupov pre monitorovanie a preskúmanie
Možné postupy pre zlepšenie	Odporúčania pre ďalšie spôsoby zaobchádzania s rizikami

Zdroj: A Risk Management Standard

Metódy identifikácie rizík sú usporiadané množiny činností (techník, procedúr), ktoré na seba logickým spôsobom nadväzujú a tvoria jednotný, vopred pripravený postup, podľa ktorého môžeme riešiť úlohy analýzy rizík. (Zánická Hollá, 2010). Na identifikáciu rizík sa využívajú najmä tieto metódy:

- ***induktívne*** *(metódy ex ante)* – analyzujú sa okolnosti, ktoré by mohli zapríčiniť ohrozenie, uvažuje sa s poruchou časti, vyhľadávajú sa tie udalosti, ktoré by mohli spôsobiť poruchu;
- ***deduktívne*** *(metódy ex post)* – sú založené na analýze udalostí, ktoré už vznikli, hľadaní a objasnení ich príčin a súvislostí medzi nimi, uvažuje sa s poslednou nehodou a vyhľadávajú sa udalosti, ktoré ju mohli zapríčiniť.

Každá jedna z metód bola vytvorená na konkrétne použitie, preto je nutné, aby sa každá z nich potrebne modifikovala.[1] V tabuľke 2 uvádzame metódy na identifikáciu rizika.

[1] https://www.ktit.pf.ukf.sk/images/clanky/Dokumenty/Projekty/Elektronicka_podpora_vyucby/Elektronick-podpora-vuby_rizik.pdf . Dostupne na internete: 26.06.2022

Tabuľka 2 Metódy identifikácie rizika

	Slovenský názov	Anglický názov	Skratka
1.	Bezpečnostný audit	Safety Audit	SA
2.	Analýza „Čo sa stane, ak…“	What if Analysis	WI
3.	Úvodná analýza nebezpečenstva	Preliminary Hazard Analysis	PHA
4.	Relatívne hodnotenie ukazovateľov nebezpečenstva	Relative Ranking	RR
5.	Štúdia nebezpečenstva a prevádzkyschopnosti	Hazard and Operability Analysis	HAZOP
6.	Analýza možnosti porúch a ich následkov	Failure Mode and Effects Analysis	FMEA
7.	Analýza možnosti porúch a kritickosti ich následkov	Failure Modes, Effects and Criticality Analysis	FMECA
8.	Analýza stromu porúch	Fault Tree Analysis	FTA
9.	Analýza stromu udalostí	Event Tree Analysis	ETA
10.	Analýza pomocou kontrolných záznamov	Check List Analysis	CLA
11.	Analýza spoľahlivosti človeka	Human Reliability Analysis	HRA

Zdroj STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod, 27. 6. 2022

Vhodným nástrojom na stanovenie ***kritérií rizík*** je vypracovanie *Matice následkov a pravdepodobností*, pričom v prvom kroku je potrebné určiť stupnicu možných následkov krízovej udalosti (tabuľka 3), v ďalšom kroku určiť hodnoty pravdepodobností, že daná udalosť nastane (tabuľka 4) a v poslednom kroku z uvedených pravdepodobností a následkov zostaviť maticu rizika tak, že výslednú hodnotu akceptovateľnosti rizika získame ako súčin hodnôt pravdepodobnosti a následku (tabuľka 5). Výsledné hodnoty následne pretransformujeme na intervaly prijateľnosti rizík (tabuľka 6).

Tabuľka 3 Matica (stupnica) následkov

	Hodnota následku	Majetkové straty	Zdravotnícke straty	Prerušenie prevádzky	Povesť organizácie	Ciele organizácie
1	**Veľmi malý**	> 5 000 €	Žiadne alebo len ľahšie zranenia.	Kritické systémy vyradené do 1 hodiny.	Zanedbateľný vplyv.	Vyriešené v každodennom riadení.
2	**Malý**	> 10 000 €	Ľahšie zranenia.	Kritické systémy vyradené na niekoľko hodín.	Nežiadúce, miestne pokrytie.	Menší vplyv.
3	**Stredný**	> 15 000 €	Zranenia.	Kritické systémy vyradené na menej ako 1 deň.	Nežiadúce, širšia medializácia.	Významný vplyv.
4	**Veľký**	> 20 000 €	Vážne zranenia.	Kritické systémy vyradené na 1 deň.	Nežiadúce, celoštátne pokrytie.	Hlavný vplyv.
5	**Veľmi veľký**	< 20 000 €	Úmrtia alebo trvalé postihnutia.	Kritické systémy vyradené na viac ako 1 deň.	Potreba informovať vládu.	Katastrofálny vplyv.

Zdroj STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod, 27. 6. 2022

Tabuľka 4 Stupnica pravdepodobnosti

	Pravdepodobnosť	Očakávané pravdepodobnosti a frekvencie udalostí
1	**Veľmi malá**	Môže nastať len vo výnimočných prípadoch.
2	**Malá**	Môže nastať raz za rok ($P^2 < 25$ %).
3	**Stredná**	Môže nastať raz za pol roka (50 % > P > 25 %).
4	**Veľká**	Môže nastať raz za 3 mesiace (75 % > P > 50 %).
5	**Veľmi veľká**	Môže nastať raz za mesiac (P > 75 %).

Zdroj STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod*, 27. 6. 2022*

Tabuľka 5 Matica rizika

Následky		Pravdepodobnosť				
		1	2	3	4	5
		Veľmi malá	Malá	Stredná	Veľká	Veľmi veľká
1	**Veľmi malý**	1	2	3	4	5
2	**Malý**	2	4	6	8	10
3	**Stredný**	3	6	9	12	15
4	**Veľký**	4	8	12	16	20
5	**Veľmi veľký**	5	10	15	20	25

Zdroj STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod, 27. 6. 2022

Tabuľka 6 Intervaly prijateľnosti rizík

Kategória	Hodnota	Charakter rizika
Neprijateľné (neakceptovateľné)	17 – 25	Vyžaduje zastavenie prebiehajúceho procesu a prijatie regulačných opatrení na jeho zníženie.
Prípustné nežiadúce (neželateľné)	12 – 16	Prípustné len v prípade, ak jeho zníženie sa nedá uskutočniť alebo je značne neefektívne.
Prípustné znesiteľné	5 – 11	Prípustné po zvážení nákladov na jeho zníženie, ak prínosy prevyšujú náklady na jeho zníženie.
Prijateľné (zanedbateľná úroveň)	1 – 4	Nevyžadujú sa regulačné opatrenia na jeho zníženie.

Zdroj STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod, 27. 6. 2022

1.2 Analýza rizika

Analýza rizika*)* sa týka ***rozvíjania*** a ***chápania rizika***. Je to proces, ktorý zahŕňa ***pochopenie podstaty rizika*** a ***určenie jeho úrovne***. Poskytuje vstup do hodnotenia rizika a rozhodnutí, či sa rizikami treba zaoberať a akú najvhodnejšiu stratégiu a metódy treba použiť. Môže poskytnúť aj vstup do prijímania rozhodnutí tam, kde treba urobiť výber a možnosti obsahujú rozličné druhy a úrovne rizika. Analýza rizika zahŕňa ***ocenenie rizika*** (odhad, výpočet). Riziko sa analyzuje *určením následkov, ich pravdepodobnosti a ďalších vlastností rizika.*

Úroveň účinnosti konkrétneho opatrenia na riadenie rizika alebo súboru súvisiacich opatrení na riadenie rizika, môže byť vyjadrená kvalitatívne, semikvantitatívne alebo kvantitatívne. Vo väčšine prípadov nie je zaručená vysoká úroveň presnosti. Môže však byť

[2] pravdepodobnosť

užitočné vyjadriť a zaznamenať mieru efektívnosti riadenia rizika, potom je možné posúdiť, či bolo vynaložené najlepšie úsilie na zlepšenie riadenia rizík, alebo potrebu poskytnutia iného spôsobu zaobchádzania s rizikom

Medzi faktory, ktoré ovplyvňujú ***pravdepodobnosť*** vzniku nebezpečnej udalosti možno zaradiť najmä napr. výstražné a varovné označenia, strážny pes, viditeľne nainštalované technické zabezpečovacie systémy (kamery, detektory a pod.) a iné opatrenia.

Medzi faktory, ktoré ovplyvňujú ***následky*** nebezpečnej udalosti možno zaradiť najmä: preventívne opatrenia, opatrenia na zníženie hodnoty aktív v jednom chránenom priestore, uloženie aktív v úschovných objektoch, havarijné plánovanie, príprava záchranných tímov a prostriedkov a pod.

Na základe spracovanej analýzy rizika pristupuje analytik v ďalšom kroku k vyhodnocovaniu rizika. V tomto kroku sa od všeobecných vlastností rizika prechádza ku konkrétnym, ktoré môžu byť určitým spôsobom exaktne vymedzené a subjektom rozhodovania (*rozhodovateľom*) je im pridelená určitá váha.

Analýza rizika sa môže realizovať *s rozličnou úrovňou podrobností* a v závislosti od samotného rizika, účelu analýzy, informácií, údajov a dostupných zdrojov. Vzhľadom k tomu, či pri vyhodnocovaní rizika charakterizujeme toto riziko číselne alebo slovne, rozlišujeme ***kvantitatívne***, ***kvalitatívne*** a ***polokvantitatívne (semikvantitatívne)*** metódy analýzy rizík. ***Ocenenie rizika*** je základným prvkom posúdenia miery rizika a následne akceptovateľnosti rizika, ktorý je použitý následne pri kontrole rizík. Na ocenenie rizík existuje veľa metód, ktoré sa používajú v rôznorodých prostrediach. Spôsob vyjadrenia o veľkosti rizika môže byť:

- slovnou deskripciou (malé, stredné, veľké),
- abstraktnou číselnou hodnotou (tzv. ordinálnou poradovou stupnicou 0 – X),
- percentuálne (tzv. kardinálnou percentuálnou stupnicou 0 – 100 %).

Kvalitatívne metódy vyhodnocovania rizík

Kvalitatívne metódy vyhodnocovania rizík sú využívané v prípadoch, kedy je náročné stanoviť interval čísel, ktorými by mohlo byť potenciálne riziko ohodnotené. Z tohto dôvodu sú v takýchto prípadoch využívané slovné hodnotenia možných hrozieb. Je však dôležité zdôrazniť, že takéto hodnotenia nie sú exaktné a vo veľkej miere závisia od vlastností subjektu rozhodovania (rozhodovateľa). *Kvalitatívna analýza sa používa najmä:*

- ako úvodný prehľad vedúci k identifikácii rizík, ktoré vyžadujú podrobnejšie skúmanie;
- tam, kde tento druh analýzy postačuje na rozhodovanie; alebo
- tam, kde číselné údaje alebo zdroje nie sú dostatočné na vykonanie kvantitatívnej analýzy.

Kvalitatívne prístupy a metódy môžu byť založené na hodnotení, ktoré využíva mnohoodborové skupiny respondentov, hodnotení špecialistov a expertov, štruktúrovaných interview a dotazníkoch.

Určenie hodnoty chráneného záujmu v štyroch slovných kategóriách – ***Malá, Nie malá, Veľká, Veľmi veľká.*** Určenie úrovne zraniteľnosti objektu v troch slovných kategóriách – ***Malá, Stredná, Veľká.*** Určenie ochranných opatrení, ktoré sú rekciou na zraniteľnosť objektu. Kategorizujú sa na – ***Veľmi účinné a Účinné.*** Príklad možného slovného ohodnotenia následkov rizika je uvedený v tabuľke 7.

Tabuľka 7 Kvalitatívne ukazovatele následkov

Úroveň	Charakteristika	Príklad
1	**Nevýznamné**	Ľahší úraz, malé finančné straty.
2	**Malé**	Ľahší úraz, stredné finančné straty.
3	**Stredné**	Nevyhnutné lekárske ošetrenie, vysoké finančné straty.
4	**Veľké**	Rozsiahly úraz, veľké finančné straty.
5	**Katastrofálne**	Smrť, enormné finančné straty.

Zdroj: Norma STN 01 01380 Manažérstvo rizika, str. 27, cit. 27. 6. 2022

Príklady možných slovných hodnotení pravdepodobnosti toho, že daná krízová situácia nastane sú uvedené v tabuľke 8.

Tabuľka 8 Kvalitatívne ukazovatele pravdepodobnosti

Úroveň	Charakteristika	Opis
A	**Takmer isté.**	Očakáva sa, že nastane vo väčšine prípadov.
B	**Asi nastane.**	Pravdepodobne nastane vo väčšine prípadov.
C	**Možno nastane.**	Niekedy by mohlo nastať.
D	**Asi nenastane**	Niekedy by snáď mohlo nastať.
E	**Sotva nastane.**	Môže nastať iba za výnimočných okolností.

Zdroj: Norma STN 01 01380 Manažérstvo rizika, str. 27, cit. 27. 6. 2022

V prípade, že máme definované jednotlivé pravdepodobnosti a prípadné následky krízovej udalosti, je možné zostaviť maticu kvalitatívnej analýzy rizika (tabuľka 9), ktorá nám určí celkovú úroveň rizika, kde:

- ***E - extrémne riziko***; vyžaduje sa okamžitá náprava;
- ***V - vysoké riziko***; treba dať do pozornosti vrcholového manažmentu;
- ***S - stredné riziko***; musí sa špecifikovať zodpovednosť manažmentu;
- ***M - malé riziko***; riadi sa bežnými postupmi.

Tabuľka 9 Matica kvalitatívnej analýzy rizika

Pravdepodobnosť	Následky				
	Nevýzmané	Malé	Stredné	Veľké	Katastrofálne
Takmer isté.	V	V	E	E	E
Asi nastane.	S	V	V	E	E
Možno nastane.	M	S	V	E	E
Asi nenastane.	M	M	S	V	E
Sotva nastane.	M	M	S	S	V

Zdroj: Norma STN 01 01380 Manažérstvo rizika, str. 27, cit. 27. 6. 2022

Pri ***semikvantitatívnych metódach*** sa pre následok a pravdepodobnosti využívajú numerické klasifikačné stupnice a kombinujú sa s cieľom stanoviť úroveň rizika s použitím vzorca. Stupnice môžu byť lineárne alebo logaritmické, alebo môžu vyjadrovať iný vzťah. Použité vzorce sa môžu tiež líšiť. Semikvantitatívne metódy využívajú najmä ***kvalitatívne popísanie stupnice, ktoré majú pridelené číselné hodnoty*****,** kombináciou týchto charakteristík sa určí hodnota rizika. Cieľom je vytvoriť stupnice, ktoré sú ***podrobnejšie,*** než môže obvykle poskytnúť kvalitatívna analýza. Cieľom nie je navrhnúť realistické hodnoty pre popis rizík, ako sa o to pokúša kvantitatívna analýza.

Kvantitatívne metódy vyhodnocovania rizík

„*Kvantitatívne metódy využívajú numerické ohodnotenie bezpečnostných rizík vyjadrením ich pravdepodobnosti, početnosti, vierohodnosti, potenciálu, dôsledkov a pod.*“[3] Použitie takýchto metód však vyžaduje dlhší časový rámec na kvalitné vypracovanie metód, a tiež vyžaduje lepšiu znalosť konkrétneho rizika. Kvantitatívne metódy na určenie veľkosti rizika využívajú dve základné hodnoty:

- *pravdepodobnosť (početnosť) vzniku udalosti,*
- *následky*, ktoré takúto udalosť sprevádzajú, alebo sú ňou spôsobované.

Základnou rovnicou výpočtu pravdepodobnosti rizika pomocou kvantitatívnej metódy je použitie základného vzorca teórie rizík, a teda:

$$R = P\,x\,N \ \text{(x s)} \tag{1}$$

kde:

- R – je veľkosť rizika systému,
- P - sú príčiny vzniku mimoriadnej udalosti, pričom $P \leq 1$,
- N - sú následky mimoriadnej udalosti (v peňažných alebo fyzikálnych jednotkách),
- s - citlivosť na zmeny.

Kvantitatívne metódy pre vyjadrenie pravdepodobnosti bezpečnostného rizika sú založené na možnosti, že sa z množiny všetkých bezpečnostných rizík prejaví iba jedno konkrétne riziko. Ak je množina bezpečnostných rizík, ktorá ma všetky riziká rovnako možné, podľa kvantitatívnej metódy sa používa pre vyjadrenie pravdepodobnosti vzťah (Hofreiter, 2002)

$$P(R_1) = \sum \frac{R_1}{R} \tag{2}$$

kde :

- $P(R_1)$- pravdepodobnosť zadaného rizika,
- $\sum R_1$ - celkový počet prípadov výskytu zadaného bezpečnostného rizika,
- $\sum R$ - celkový počet všetkých výskytov bezpečnostných rizík.

Ďalšou spomínanou možnosťou, ako sa pomocou kvantitatívnej metódy dá vyjadriť bezpečnostné riziko je početnosť. Početnosť nám vyjadruje aká je intenzita výskytu zadaného rizika za určenú časovú jednotu. Je vyjadrená ako (Hofreiter, 2002):

$$R_i(t) = \frac{\sum R_i}{t} \tag{3}$$

kde:

- Ri (t)- početnosť rizika Ri za určenú časovú jednotku,
- $\sum$ Ri - celkový počet výskytov rizika Ri,
- t - určená časová jednotka (mesiac, deň, hodina a pod.).

$$D(R_i) = \frac{S(R_i)}{\sum A} \tag{4}$$

kde:

- D(Ri)- dôsledok bezp. rizika Ri, vyjadrený ako koeficient, z intervalu <0, 1>,

[3] HOFREITER L., Bezpečnostný manažment, s. 75, cit. 18. 1. 2018, 12:58

- S(Ri)- veľkosť škody, ktorá môže byť spôsobená bezp. rizikom Ri, (vyjadrená vpeňažných jednotkách),
- ∑ A - celková hodnota aktív (vyjadrená v peňažných jednotkách).

Komplexné vyjadrenie bezpečnostných rizík v numerickom tvare (Hofreiter, 2002):

- pre (jedno) bezpečnostné riziko:

$$R = P(R).\ D(R) \tag{5}$$

- pre (n) bezpečnostných rizík:

$$R_c = \sum_{i=1}^{n} P(R_i)\ .D(R_i) \tag{6}$$

kde:

- R – číselná hodnota celkového rizika,
- P(Ri) – pravdepodobnosť rizika (Ri),
- D(Ri) – hodnota dôsledkov na riziko (Ri),
- N – počet uvažovaných bezpečnostných rizík.

S realizovanými bezpečnostnými opatreniami (Hofreiter, 2002):

$$R = P(R).\ D(R).\ Ko \tag{7}$$

kde:

- Ko – koeficient pre kvalitu a efektívnosť realizovaných ochranných opatrení. Numerické vyjadrenie koeficientu závisí od prevedenia ochranných opatrení, a môže dosahovať hodnoty:
- $0 \leq Ko < 1$ – bude platiť, ak budú realizované ochranné opatrenia,
- Ko= 1 – bude platiť, ak nebudú realizované žiadne opatrenia,
- Ko>1 – ak opatrenia nebudú zabezpečovať funkciu ochrany, ale budú spôsobovať zvyšovanie škody pre subjekt.

Hodnoty koeficientu ochranných opatrení (Hofreiter, 2002):

Slovné vyjadrenie	**Hodnota Koi**
Vysoko účinné	0 ÷ 0,2
Významné	0,21 ÷ 0,4
Základné	0,41 ÷ 0,7
Nepatrné	0,71 ÷ 0,99

V prípade použitia kvantitatívnych metód vyhodnocovania rizík je nesmierne dôležité podotknúť, že aj v prípade dôkladnej analýzy výskytu možných rizík sa v prípade celkovej pravdepodobnosti jedná len o odhad, v žiadnom prípade nie o exaktnú hodnotu pravdepodobnosti vzniku rizikovej udalosti a jej prípadných následkov.

Kvantitatívne metódy sú založené na matematickom výpočte rizika z pohľadu frekvencie výskytu hrozby a jeho dopadu. Tieto metódy sú viac exaktné než kvalitatívne. (Smejkal, Rais, 2003, str.85) Ich použitie vyžaduje viac času a úsilia. Tieto metódy sa dajú použiť predovšetkým v tých prípadoch, ak je dostatok relevantných údajov, ktoré sa dajú hodnotiť štatisticky – používajú sa najmä v oblasti bezpečnosti organizácií a ich informačných systémov. Hodnotiteľ môže byť zahltený množstvom dát, z ktorých nie všetky sú potrebné danú analýzu. Patria sem:

- *Risk PAC* – automatizácia dotazníkových postupov, riziká sa stanovia na základe spracovania vyplnených dotazníkov.
- *Risk Watch* – programový produkt s metodickým súborom pre zistenie, simuláciu a nasledovnú zmenu parametrov jednotlivých rizík systému. Forma spracovania výsledkov získaných zo súboru otázok.

- *CRAMM* (CCTA Risk Analysis and Management Methodology) – táto metóda hodnotí jednotlivé činnosti pričom vychádza z modelu systému, ktorý už bol zostavený. Tieto činnosti spája do logických skupín, následne skúma možné hrozby, ktoré pôsobia na skupiny a posudzuje ako je bezpečný celý systém. Výsledky, ktoré sa dosiahnu porovnáva so zavedenými systémovými opatreniami na zníženie rizík. Stanovia sa požiadavky na základe čoho sa navrhnú bezpečnostné opatrenia.
- *COBRA*
- *@RISK* – využíva simulačné metódy Monte Carlo, údaje sú spracovávané do tabuľkovej formy, pričom hodnoty, ktoré nemôžme presne stanoviť sú nahradené funkciami.
- *Metóda MOSAR – pre systematickú analýzu rizík (Method Organized for Systematic Analysis of Risks)* - celkový prístup v desiatich krokoch, systém rozdeľuje na menšie podsystémy následne sa identifikujú ohrozenia, ktoré sa zapíšu do prvej tabuľky. Druhá tabuľka sa zameriava na primeranosť bezpečnostných opatrení. Tretia tabuľky uvádza vzájomnú závislosť prvých dvoch, z ktorej vychádzajú potencionálne nebezpečné poruchy. Následne sa spracuje scenár. Bezpečnostné opatrenia sú následne usporiadané do logického stromu a zostatkové riziká sa analyzujú na základe dohodnutých pravidiel.
- a iné.

Proces analýzy rizika začína ***určením pravdepodobnosti***, že riziko bude mať hmotné následky. Určenie pravdepodobnosti výskytu udalosti je zásadný problém v oblasti hodnotenia rizík, pretože štatistické údaje nie sú k dispozícii pre všetky druhy minulých udalostí. Určenie pravdepodobnosti môžu podporovať nasledujúce otázky:
- Vyskytli sa tieto udalosti už v minulosti, alebo je to ojedinelý výskyt?
- Vyskytujú sa takéto udalosti aj v iných zariadenia a súčastiach?
- Koľko ľudí je touto udalosťou ohrozených?
- V akom časovom rozsahu sa podozrivé vybavenie alebo problematický postup používa?
- Aké sú tam organizačné, administratívne alebo regulačné následky, ktoré by mohli spôsobiť väčšie ohrozenie verejnosti?

Pri ***analýze následkov*** sa určuje ***povaha a druh následku***, ku ktorému by mohlo dôjsť za predpokladu, že došlo k zvláštnej situácii alebo udalosti. Udalosť môže mať *množstvo rôznych veľkostí následkov* a môže *ovplyvniť množstvo rôznych cieľov a rôzne zúčastnené strany*. Udalosti môžu mať:
- nízky následok, ale s vysokou pravdepodobnosťou,
- vysoko závažný následok a nízku pravdepodobnosť,
- nejaký stredný výsledok.

Následky sa môžu vyjadriť v termínoch hmotných alebo nehmotných následkov (finančných, technických, zdravotných alebo iných). V niektorých prípadoch sa pre vyjadrenie následkov a ich pravdepodobnosti v rozličnom čase, v rozličných miestach a situáciách a pre rozličné skupiny vyžaduje viac ako jedna numerická hodnota. Posúdenie závažnosti následkov udalosti (vplyv) je často veľmi ťažké pre dlhodobý nehmotný majetok, ďalšia otázka, ktorú treba riešiť je ocenenie aktív. Pri hodnotení následku môžu nastať ujmy:
a. úmrtie/zranenie – zamestnanci, návštevy, okoloidúci, široká verejnosť,
b. škoda – aká je veľkosť škody na majetku alebo poškodenia vybavenia,
c. prerušenie činnosti – prevádzky, systémov IKT, iných činností,
d. poškodenie povesti,
e. nesplnenie cieľov,
f. iné ujmy.

Hlavným výstupom analýzy rizika je ***zoznam príležitostí*****,** ktoré sa musia sledovať (podnikateľské riziká), ***nebezpečné udalosti*** (ohrozenia, bezpečnostné riziká), ktoré vyžadujú

pozornosť, zdokumentované ***zdroje rizík,*** zdokumentované ***faktory, ktoré ovplyvňujú následky a pravdepodobnosť***.

Hodnotenie rizika

Účelom hodnotenia rizika je pomôcť pri prijímaní rozhodnutí o rizikách, vyžadujúcich zaobchádzanie a priorite pre zavedenie zaobchádzania. Hodnotenie rizika zahŕňa:

- *porovnanie veľkosti rizika* zistenej v procese analýzy, s kritériami rizika určenými počas vytvárania súvislostí,
- zváženie *potreby* zaobchádzania s rizikom,
- vydanie rozhodnutia o rizikách, ktoré vyžadujú zaobchádzanie,
- *určenie priorít rizík*, ktoré vyžadujú zaobchádzanie.

Rozhodnutia majú brať do úvahy širší rámec rizika a musia zahŕňať úvahy o tolerancii rizika pre iných účastníkov, ako je organizácia, ktorá má z rizika osoh. Rozhodnutia sa majú prijať v súlade s požiadavkami zákonov, predpisov a s ďalšími požiadavkami. V niektorých prípadoch vyhodnotenie rizika môže priviesť k rozhodnutiu vykonať ďalšiu analýzu alebo zachovať jestvujúce opatrenia na jeho kontrolu a nezaoberať sa rizikom nijakým iným spôsobom (takéto rozhodnutie ovplyvňuje prístup organizácie k riziku a k určeným kritériám rizika).

Bežný spôsob spočíva v rozdelení rizík na tri skupiny:

a. *horná skupina*, kde je úroveň rizika považovaná za neprijateľnú, bez ohľadu na to, či činnosť môže znamenať akýkoľvek prínos, a zaobchádzanie s rizikom je nevyhnutné za akúkoľvek cenu,
b. *stredná skupina*, kde sa berú do úvahy náklady i prínosy, a príležitosti sú zvažované vzhľadom na potenciálne následky,
c. *dolná skupina*, kde je úroveň rizika považovaná za zanedbateľnú alebo tak malú, že nie sú potrebné žiadne opatrenia na zaobchádzanie s rizikom.

Na posúdenie nákladov a prínosov vybraných spôsobov zaobchádzania s neprijateľnými i prípustnými rizikami sa využíva ***zásada ALARP***, ktorá ukazuje, že riziku, riadeniu rizika a modifikácii rizika je potrebné venovať primeranú pozornosť. Zásada zahŕňa zváženie a porovnanie úrovne rizika s ťažkosťami, časom a finančnými nákladmi, potrebnými na jeho riadenie.

Výstupom hodnotenia rizík je Zoznam rizík, ktoré vyžadujú zaobchádzanie podľa priorít pre zaobchádzanie. Na základe určených priorít je stanovené poradie rizík na voľbu spôsobov (u) zaobchádzania s nimi. Obsah problematiky posudzovania rizika je súhrnne uvedený v tabuľke 10.

Tabuľka 10 Obsah problematiky posudzovania rizika

POSUDZOVANIE RIZIKA		
IDENTIFIKÁCIA RIZÍK	**ANALÝZA RIZÍK**	**HODNOTENIE RIZÍK**
Proces hľadania, spoznávania a popísania rizika	Proces na pochopenie povahy, zdrojov a príčin rizík pre ocenenie úrovne rizika	Proces porovnania výsledkov analýzy rizík s kritériami rizika
Zahŕňa identifikáciu	**Zahŕňa posúdenie**	**Zahŕňa**
• **zdrojov rizika** – prvkov, ktoré samy osebe alebo v kombinácii majú vnútorný potenciál vyvolať riziko a oblasti ich následkov, • **udalostí,** ktoré zdroje rizika môžu spôsobiť, • **okolností,** ktoré by mohli mať potenciálne následky na dosiahnutie cieľov, • **príčin rizika** – toho, ČO sa môže stať, KEDY a KDE, PREČ O a AKO sa to môže stať, • **potenciálnych následkov,** • **opatrení** zavedených na modifikáciu rizika	• **príčin a zdrojov rizika** – pozitívne vlastnosti, nebezpečenstvo (*príležitosť, ohrozenie),* • **kladných a záporných následkov udalosti** – *zisk, ujma,* • **pravdepodobnosti,** že tieto následky môžu nastať, • **ďalších vlastností rizika** – *faktory, ktoré ovplyvňujú následky a pravdepodobnosť*	• **porovnanie úrovne rizika** zistenej v procese analýzy, **s kritériami rizika** určenými počas hľadania súvislostí, • **zváženie potreby zaobchádzania s rizikom**, • **vydanie rozhodnutia** o prijateľnosti resp. neprijateľnosti či prípustnosti rizika
Zoznam rizík	Zoznam **príležitostí** a **nebezpečných udalostí,** Zdokumentované **zdroje rizík** a **faktory, ktoré ovplyvňujú následky a pravdepodobnosť**	**Rozhodnutie o prijateľnosti, neprijateľnosti či prípustnosti rizika**

ZÁVER

Problematika posudzovania rizík je v súčasnosti aktuálna, zaoberá sa ňou veľké množstvo manažérov na riadiacich funkciách s cieľom eliminovať rizika, ktoré môžu zásadne ovplyvňovať všetky procesy v organizácii. Nevyhnutný predpoklad na vykonanie posudzovania rizika prestavuje určenie súvislostí. Dôraz kladieme na etapu identifikácia rizika, pretože len riziká, ktoré identifikujeme môžeme ďalej analyzovať a v konečnom dôsledku modifikovať.

GRANTOVÁ PODPORA

Príspevok bol podporený výstupmi riešenia výskumného projektu *NI 4200549 Optimalizácia rozhodovacích procesov krízového manažmentu v podmienkach OS SR pri predchádzaní a riešení krízových javov nevojenského charakteru.*

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BELAN, Ľ. 2015. *Bezpečnostný manažment – Manažérstvo rizika*. Žilinská univerzita v Žiline/EDIS – vydavateľstvo Žilinskej univerzity. 201 s. ISBN 78-80-554-1163-7

BUGANOVÁ K., LUSKOVÁ M. 2011. *Analýza rizík v podniku metódou FMEA.* In: Krízový manažment 1/2011, vedecko-odborný časopis. Žilina: Žilinská univerzita, Fakulta špeciálneho inžinierstva. ISSN 1336-0019.

IVANČÍK, R. 2021. *O potrebe teórie bezpečnosti*. In: Vojenské reflexie – vojenský vedecký časopis 2/2021. Liptovský Mikuláš: Akadémia ozbrojených síl gen. M. R Štefánika. s.39-53, ISSN 1336-9202

RATTNER, D. 2010: *Risk Assessments.* Security Management. Northeastern University, Boston. 15 Mar. 2010. Lecture.
HOFREITER, L, 2002. *Bezpečnostný manažment*. Žilina: EDIS, 2002. ISBN 80-7100-953-9
SMEJKAL Vladimír, RAIS Karel, *Řízení rizik*, 1. vyd. Praha: Grada Publishing a.s., 2003. str. 85.
VARCHOLOVÁ T., DUBOVICKÁ L., Nový manažment rizika, 1. vyd. Bratislava: Iura Edition, 2008. str. 70
ZÁNICKÁ HOLLÁ K. 2010. *Posudzovanie rizík priemyselných procesov*. Bratislava, 2010. ISBN 978-80-8078-344-0
A Risk Management Standard (Štandard manažérstva rizika podľa Inštitútu manažérstva rizika, Londýn).
STN ISO 31000 (01 0381): 2019, Manažérstvo rizika. Návod
ISO/IEC 27005:2011 – *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*
STN EN 31010:2011 – *Manažérstvo rizika, Metódy posudzovania rizika.*

doc. Ing. Lubomír BELAN, PhD.
Katedra logistického zabezpečenia, Akadémia ozbrojených síl gen. M. R. Štefánika
Liptovský Mikuláš
lubomir.belan@aos.sk

Ing. Ján MIŠÍK, PhD.
Ministerstvo spravodlivosti Slovenskej republiky
Račianska 71
813 11 Bratislava
jan.misik@justice.sk

THE ROLE OF COMMANDERS' CBRN PROFICIENCY DURING THE PERIOD OF PLANNING AND EXECUTING MILITARY OPERATIONS

Tamás BEREK

ABSTRACT

The identification and attacking our centre of gravity can be a component of the adversary's operation planning. The enemy's „indirect approach" when attacking our centre of gravity by concentrating on utilising the physical and moral or other crucial vulnerability of our forces involves efforts which would eventually lead the enemy to overcome the centre of gravity. CBRN[1] defence is one of these crucial points. Besides fully completing the goals the commander should try and hide or eliminate these vulnerabilities by appropriate risk management based on threat analysis and the coordinated implementation of the regulations concerning the protection of the troops. The commander should be able to plan operations in the CBRN environment by keeping the chemical, biological and radiological exposure at the lowest possible level and by the ALARA[2] principle, bearing in mind threats and the different operational abilities of the subordinated subunits. The CBRN threat to the timely and accurate assessment of the evaluation of the information of major importance. In these days the commanders and their staffs needs the specialist CBRN defence capabilities in support of the operations when operating under the threat of the use of CBRB weapons or in the CBRN environment. The commanders' appropriate CBRN defence proficiency is vital in order to success of mission in the CBRN environment.

Keywords: CBRN threat, CBRN defence, CBRN expertise

INTRODUCTION

As a result of the earlier NBC arms race security policy specialists designated the threat arising from the proliferation of materials, tools and intellectual products needed to produce CBRN weapons as a new type of hazards. CBRN devices that got out of control and enlarge the repository of small armed groups could play a role in smaller local wars. In spite of the fact that only a fraction of terrorist acts committed in the past 25 years proved to be CBRN incidents the expansion of international terrorism could give cause for concern. Due to the growing capabilities of international terrorism the utilisation of radiological, chemical and biological materials in acts of terrorism represents a typical component of the scenarios of exercises testing the reliability of defence systems worldwide.

In he course of preparing armed forces CBRN environments as a possible theatre of armed fights should be taken into account in the future, too. Soldiers should be prepared so that they can continue military activities under CBRN conditions also. One of the conditions is to establish skills that enable soldiers to first of all survive CBRN impacts and to continue the activities.

Factors occurring not as a direct result of the application of CBRN weapons (e.g. the discomfort, heat stress, dehydration and respiration difficulties during sustained periods of individual protective equipment wear) but related to CBRN impacts occurring in real CBRN

[1] CBRN: Chemical Biological ,Radiological, Nuclear
[2] As Low As Reasonably Achievable

situations (penetrating radiation exposure, incorporation of radioactive materials, intoxication, infection by biological agent) deteriorate the survival ability of the soldier.

The direction of changes in the warfare procedures is unforeseeable; conclusions can only be drawn from the trends of development of sciences, technology and military theory. According to the concepts of security experts the warring parties would not represent equal forces since the adaptation of the state-of-the-art technology is not even possible for all modern armed forces. Asymmetric warfare that obviously intends to counterbalance dominance will presumably move towards applying CBRN tools.

It is of no avail for combat units to possess the most advanced regular CBRN protection gear if the components that enable the commander to employ them in an CBRN environment in order to execute certain tasks are missing from the preparation scheme.

Preparations and military trainings should follow the changes of military theories since armed forces prepared for current challenges and currently preparing themselves for future threats can represent combat-ready forces under the changed circumstances of wartime environment. And it is reasonable to state that every penny spent on the training, equipment and armaments of officer candidates is just wasting money if we are unable to protect these combat forces for survival.

That's why personnel's CBRN defence familiarity should be of high priority.

With regard to the technical devices of CBRN defence subunits the technical change that has occurred in the past decade and the changes still occurring are noticeable in the field of chemical, radiological and biological reconnaissance, chemical and radiological decontamination and personal protection (individual protective equipment).

Devices that have recently become regular have parameters that are different from the previous ones but the deployment of entirely different technologies must also be taken into account. The changing of technical assets meant – among others – changing quality also, with regard to the followings.

By the improvement of the CBRN detection ability and handling of chemical and radiological detectors and the reduction of sensitivity to interference, detection threshold and detection time as well as with computer connectivity chemical and radiological reconnaissance became more accurate.

When performing certain chemical and radiological reconnaissance missions infrared spectroscopy based devices could also play a role.

The improvement of positioning accuracy by using and putting in service modern positioning systems (GPS) significantly contributed to the modernisation of aerial and ground radiological reconnaissance.

The new types of individual protective equipment the requirements of ease of wearing better, which has an effect on carrying out training and tasks under real or supposed CBRN circumstances mainly because the period of applicability of the individual protective equipment increased. These features as well as the sensitivity of the technical components and the sensitive technical devices of the command and control (C2) system to decontamination substances in service involve changes (mainly in respect of the activities of the CBRN subunits) the knowledge of which has substantial influence on the planning and execution of military operations.

1 THE EFFECTS THE CBRN ENVIRONMENT ON MILITARY OPERATIONS

The complexity of the CBRN environment of military operations makes it difficult to assess the operation area as well as to plan and execute the operations since besides the deployment of any CBRN weapon components their combined and/or consecutive deployment can also be expected. (Berek, 2011)

As a result of an incidental nuclear strike (which can also be a planned strike of the allied forces) the CBRN situation is characterised by terrain highly contaminated with radioactive nuclides, fires, obstacles, destruction and airspace contaminated with radioactive compounds as a result of the complex effect of the nuclear strike. These circumstances make it considerably difficult to continue the military operation, the development of tactical success and last but not least the activities of the troops eliminating the consequences of the strike.

As a possible tool of terrorist acts with regard to radiological devices security experts most frequently specify improvised radioactive exploding devices (IRDE) as alarming sources of hazard. The consequences can have an indirect effect on military operations. Because of surveying and decontaminating military facilities of important strategic and operational significance (among others logistic facilities, harbours, march and supply routes) following contamination and because of the implementation of protection measures essential operations may be delayed.

However, considering tactical consequences the prospects are even worse. In the operational area of these forces the operational ability may suffer in the areas affected by radiological hazard.

In addition to deploying biological warfare agents and weapons at theatres of war by the enemy a possible source of hazard originating in hazardous biological substances getting into the environment could be an attack against facilities – or their secondary destruction – where infectious materials are produced or stored.

Military hazards or hazards of civilian purposes represent the chemical environment.

In addition to the threat posed by chemical warfare the chemical hazards developing as a result of the unintended destruction of facilities containing hazardous materials by traditional weapons (or their destruction not due to a strike) should also be considered.

Discharge in the area affected by the conflict may have an impact on the course of operations regardless of the fact whether it originates in intentional activity or an accident. The CBRN environment of military operations determines that future military operations must be planned and conducted by taking into account the risk of the deployment of CBRN weapons against the forces participating in these operations. Consequently these forces should not only be capable of providing protection against traditional attacks but they should also be familiar with conducting operations in an CBRN environment for a lengthy period.

2 COMMANDERS' KNOWLEDGE IN ORDER TO UNDERSTAND HEALTH EFFECTS OF WEARING INDIVIDUAL PROTECTIVE DEVICES

The commander's staff is to continuously analyse the CBRN threat according to the recommendations of the CBRN defence officer, to analyse the dress states of the related protective wear and to operate the CBRN warning and reporting system. As formulated in the CBRN defence doctrine the purpose of the CBRN warning and reporting is to warn the troops in time of the CBRN strikes or incidents, and to provide the commander with timely and accurate information for the assessment of the effects CBRN incidents have on military operations.

Depending on the CBRN situation the commander is forced to take actions that decrease the effective forces' combat effectiveness and morale and through that may endanger that the goal set by the commander is achieved. For exactly that reason when relieving dress levels stipulated for the individual protective equipment of his subunit being in an CBRN environment the commander has to continuously consider – beside several factors – the expected damage to the health and the survival opportunities even if it is not possible to know in advance whether taking the additional risk would have resulted in success.

The evaluation of applying individual protective equipment should appear at all commanding levels as part of the METT-T (mission, enemy, terrain, troops and time) assessment.

When establishing a high CBRN threat level the dress state of the personal equipment can be ordered within a very broad range, based on the decision of the subunit commander.

Connecting this directly to the theory of „mission command", according to which commanders provide their subordinates with appropriate operational efficiency and the freedom of movement to seize and retain the initiative, this means that the decision concerning the dress state of the protective wear should be made at the subunit commanding level!

The purpose of the impact analysis of the dress states of the protective wear is that the commander finds the balance between the losses occurring due to the effects of wearing the individual protective equipment after the real CBRN threats are explored and the success of mission execution in such a way that he determines (through determining the performance degradation factor that occurs at the applied dress states of the IPE) the expected increase of time required to execute the mission, the expected water requirement – by taking into account the loss acceptable for the success of the tactical mission. The evaluation process of the dress states applied for the protective equipment provides information also about the expected losses of personnel due to weather parameters (temperature, humidity), the nature of the activities during mission execution, the applied protection level of the protective equipment, and – without easing – the estimated water loss. After analysing the expected gains/risks the operational commander decides on the withdrawal of the units from the battlefield or on the continuation of the combat activity.

3 CBRN RECONNAISSANCE IN THE SYSTEM OF THREAT ASSESSMENT

In the course of operational planning and elaborating the CBRN defence plan (which is part of the operational order), when assessing the impacts of the CBRN protective measures on the combat effectiveness and the combat procedures of our own troops as well as when the CBRN defence staff are planned and the conditions for fulfilling them are specified the most important thing is to use reliable and accurate data.

The chemical and radiological reconnaissance of the company performed in its own interest (major barracks, firing positions, march lines) at a low level of CBRN threat is basically planned by the CBRN defence NCO of the company. In addition the deployment of the organisational and non-organisational CBRN defence subunits should be coordinated by the CBRN defence staff officer.

The primary information about the chemical and radiological reconnaissance tools put in place for all subunits provide initial information about the use of the CBRN weapons deployed in the field. However, the CBRN reconnaissance ordered for the more accurate identification and delimitation of the contaminated area is a lengthier procedure.

From the aspects of sample collection, transportation and exploration, as well as considering other aspects the application of the field (mobile) version of the CBRN defence analytical laboratory, providing the ability of „unambiguous identification", would be ideal in operational areas, and is also necessary, bearing in mind that it can be installed in a not too big but still secure distance from the zone of military operations, in order to provide information quickly. However, as a first step it is necessary to establish a trained sampling group equipped with the tools suitable for the sampling procedures. (Berek, 2011)

In addition to sampling the reconnaissance ability of the CBRN defence support platoon supports the commander's assessment of the situation by providing basic data for the assessment of the impact of chemical, biological, radiological and nuclear substances on the

operational area and on the operation, following the identification of the CBRN hazard, to the specified extent of basic abilities

4 THE COMMANDER'S EXPECTED CBRN DEFENCE EXPERTISE

With respect to commanders the requirements of the CBRN proficiency3 order that commanders should have CBRN defence knowledge that exceeds the knowledge of his subordinates. In order that the commander can plan and execute the operation in the surroundings of hazardous facilities or in an CBRN environment originating from an attack, the hazards of chemical, biological and radiological contamination events, originating from CBRN strike or of non-strike, must be known.

Regarding the efficiency of warning and reporting the interpretation of the CBRN reports is extremely important as well as the knowledge of the rules of warning and reporting, together with the application ability of the CBRN defence regulations.

On the other hand the whole series of CBRN defence measures make it difficult to properly accomplish missions. The time required increases and in addition it lays considerable psychic burden on the personnel.

The commander can only accomplish the specified tasks and obligations efficiently if he involves top position persons of his staff and their staffs as well as the units subordinated to them in the accomplishment of professional activities. By stressing „reliability" as one of the demands made on the methods of making the decision, which means the authenticity of the material processed, the accuracy of the procedures developed and their professional acceptability and feasibility, it can be stated that the basic requirement of reliability is the professional skills of the staff, grounded information and the CBRN skills of the staff. During operations the control of the intelligence preparation of the battlefield and during the preparation and conduct of the military operation the collection, analysis and evaluation of data that concern the enemy and influence the enemy's activities has great importance for the commander to make his decision, thus e.g. the role of the intelligence- (G2) and the operation-section (G3) is vital concerning the expected deployment of CBRN weapons. (Hajdú et al, 1999)

Operational activities may not only be implemented in the course of combat operations but also during non-combat operations. The handling and assessment of the CBRN situation is a very complex task when providing CBRN defence support both in case of high4 CBRN threat level and in case of real CBRN situation developed as a result of the deployment of weapons of mass destruction. Therefore gathering information from the area of operation should be implemented through the coordinated efforts of the forces performing complex reconnaissance activity. In the assessment of the situation the reconnaissance and assessment system has the task of evaluating the threat induced by the CBRN weapons that can be deployed by the adversary (enemy) and size up the consequences on the one hand, and to size up the possibility of the expected contamination as a result of the destruction of industrial facilities storing toxic industrial materials in the area of operation, on the other.

The CBRN threat level – among many other factors – significantly influences the efficiency and successfulness of the activities carried out in the operational area.

When planning military operations and during the process intelligence preparation of the battlefield it is of extreme importance to determine the current and overall CBRN threat – together with the industrial sources - affecting the area of operation and activities. The basic aim of the CBRN IPB is to provide information for the commander's Priority Intelligence

[3] ATP 3.8.1

[4] The highest threat level specified by NATO STANAG 2984

Requirements (PIRs) which is the first stage of the commander's operation planning process. Intelligence Preparation of the Battlefield generally precedes the mission analysis and the commander's operation planning process. Specifically the preliminary forecast of the CBRN circumstances must be prepared which forms the basis of further reconnaissance and operation planning. Thus the CBRN IPB should include – among others – the evaluation of the CBRN threat, the theatre of military operations, the allied forces and the meteorological assessment.

The commander of the joint forces is responsible for determining the CBRN threat level but commanders at all levels should determine the physical CBRN protection level. In order to determine the threat the CBRN threat status must be assessed and continuously updated. When developing abilities the possible CBRN hazards, threats and the risks of an incidental industrial release should be taken into consideration. By taking into account CBRN risks the CBRN defence capacity of our own forces should be determined with special regard to individual protective devices as well as the capacity of the CBRN defence specialists. All that should form the basis of evaluating own forces. The positioning of the forces is ideal if combat effectiveness does not decrease significantly even in an environment with many CBRN hazards. When planning the operations the areas endangered by the release of hazardous industrial substances (Toxic Industrial Materials) should be avoided by keeping in mind the principle of avoiding hazard except if these areas cannot be passed around from an operational aspect and are especially important in the course of the operation.

In order to determine the threat the CBRN threat must be assessed and continuously updated. The commander should be aware of the abilities of his subunits and for this purpose he has to evaluate the CBRN defence capacity of the subordinated organisations from the aspect of surviving CBRN strikes and the successful continuation of the operations in an CBRN environment. The assessment of the CBRN defence abilities should be performed in the light of the CBRN defence organisation and the CBRN protection gear put in service. The CBRN defence officer performs essential duties during this assessment. Furthermore, the commander has to ensure that the exercises and training executed to obtain the essential individual CBRN proficiency of the personnel are in line with the NATO and the national principles.

CONCLUSION

The commander is responsible for organising CBRN defence in accordance with the duties of the CBRN defence of the troops. The efficient application of the CBRN defence regulations ensuring survival could guarantee protection in the period of assuming CBRN risks. At the same time there is the requirement of understanding the philosophy and consequences of assuming risks, obtaining accurate and authentic information about the CBRN circumstances and the evaluation and managing of risks. The commander's adequate CBRN defence proficiency is a pledge of that.

The staff should perform a huge number of tasks in the course of decision-making. The selected method should comply with numerous requirements in order to enable the staff to perform these tasks in time and with the appropriate contents.

The commander's requirement for crucial information makes it possible to direct the staff's efforts in the course of obtaining the information for making the decision which enables more efficient operation planning.

In order that the commander can put into words with tolerable accuracy his requirement for information on the CBRN circumstances towards his staff he should be aware of the effects of CBRN weapons on the theatre of military operations as well as of the effects directly or indirectly affecting combat activity.

BIBLIOGRAPHY

Berek, Tamás 2011: NBC (CBRN) analytical laboratory as a special CBRN capacity supporting operations, Hadmérnök http://www.hadmernok.hu/2011_1_berek.pdf

Berek, Tamás 2013: Key elements of standards of proficiency for CBRN defence in military officers' education, Hadmérnök, Volume VIII, Issue 4. – December 2013, ISSN1788-1919 http://www.hadmernok.hu/134_04_berekt.pdf

Hajdú I. - Somorácz A. - Szabó Gy. - Balogh Z. - Bíró B. - Fodor J. - Téglási J. - Horváth A. - Magyar I .: Staff service, textbook ZMNE, Budapest, 1999

NATO: ATP-3.8.1 vol. III. CBRN Defence Standards for Education, Training and Evaulation 2011 Online: https://standards.globalspec.com/std/1560093/ATP-3.8.1%20VOL%20III

NATO: ATP-3.8.1 vol I. CBRN Defence on Operations 2010 Online: https://standards.globalspec.com/std/14507150/atp-3-8-1-vol-i

Nuclear, biological and chemical defence doctrine 2010 MH ÖHP publication

Dr. Tamás BEREK
University of public service
Hungary
berek.tamas@uni-nke.hu

BUDOVANIE PARTNERSTVA EÚ A NATO

BUILDING A PARTNERSHIP EU AND NATO

Ivan BYSTRIANSKY

ABSTRACT

The common strategic interests of the North Atlantic Treaty Organizationand the European Union create a basis for mutual cooperation with a focuson crisis management and capacity development, which are implemented through mutual political consultations. Part of the cooperation is also the provision of support to their common partners in the Eastern and Southern Neighbourhoods. However, these two different organizations share many common members, shared values and face the same security threats and global challenges. Their mutual cooperation takes place in a spirit of complete openness and transparency and with full respect for the decision-making independence and decision-making procedures of both organizations. This cooperation is based on the principles of inclusiveness and reciprocity, without prejudice to the specific nature of the security and defense policy of any of their member states.

Key Words: cooperation, security, capacity,

ÚVOD

Európska únia (ďalej len „EÚ“) je politická organizácia s civilno-vojenskými štruktúrami, ktorá vznikla na základe medzivládnej dohody jej členských štátov za účelom hospodárskej, politickej a kultúrnej spolupráce a ako nástroj na riešenie spoločných problémov v oblasti vnútornej, ako aj zahraničnej politiky. Jeden z mnohých kľúčových princípov, ktoré EÚ rozvíja je aj *Spoločná zahraničná a bezpečnostná politika*[1] (ďalej len „SZBP“), ktorá prešla od svojho založenia *Maastrichtskou zmluvou*[2] z roku 1993 viacerými zmenami a neustále sa rozvíja.

Rozhodujúcim zlomom novodobých dejín Európy bola vojna v Juhoslávii. Členské štáty *Západoeurópskej únie*[3] (ďalej len „WEU“ - Western European Union) neboli schopné rýchlo a účinne reagovať na prebiehajúci ozbrojený konflikt, čo vyvolalo diskusiu o potrebe disponovania autonómnou vojenskou silou WEU, nezávislou na Spojených štátoch a ktorá by v rámci *druhého piliera EÚ*[4] podporovala SZBP. Potrebná akčnosť a flexibilnosť SZBP bola dotvorená Amsterdamskou zmluvou, uvedenou do platnosti v roku 1999. K už zavedeným nástrojom SZBP, a to spoločný postoj, spoločné akcie, vytvorila Amsterdamská zmluva nový

[1] Prispieva ako druhý medzivládny pilier Maastrichtskej zmluvy k cieľom EÚ zachovávať mier, posilňovať medzinárodnú bezpečnosť, podporovať medzinárodnú spoluprácu, ako aj rozvíjať a upevňovať demokraciu, právny štát a dodržiavanie ľudských práv a základných slobôd.

[2] Nazývaná aj ako Zmluva o Európskej únii, ktorá vstúpila do platnosti po ratifikovaní všetkými členskými štátmi 1.11.1993 a od tohto obdobia hovoríme o vzniku Európskej únie.

[3] Bola medzinárodnou organizáciou, vojensko-politickým zoskupením desiatich západoeurópskych krajín vytvorená v roku 1954 reorganizáciou Bruselského paktu s perspektívou spojeneckého zväzku členských krajín vtedajších Európskych spoločenstiev so sídlom v Londýne.

[4] Definovaný v Maastrichtskej zmluve ako oblasť SZBP.

nástroj v podobe spoločnej stratégie a určila úlohu inštitúcií EÚ pri jej formulovaní (Harvánková, 2016, s.18).

Významnou udalosťou, ktorá ovplyvnila tvorbu európskej spoločnej stratégie, bolo rozšírenie členov EÚ v roku 2004, kedy bol počet členov výrazne navýšený. Preto logicky bolo potrebné realizovať reformy Maastrichtskej zmluvy, ktoré nakoniec vyústili v prijatie Lisabonskej zmluvy. Lisabonská zmluva z roku 2009 so sebou priniesla radu reforiem v oblasti SZBP, ktoré podporili angažovanosť EÚ na medzinárodnej scéne. Jednalo sa o vytvorenie funkcie Vysokého predstaviteľa EÚ pre zahraničné veci a bezpečnostnú politiku, ktorý reprezentuje stanoviská EÚ v danej oblasti a vytvorenie novej inštitúcie Európskej služby pre vonkajšiu činnosť (EEAS – European External Action Service), ktorej prioritnou úlohou je poskytovanie odbornej pomoci Vysokému predstaviteľovi EÚ pre zahraničné veci a bezpečnostnú politiku pri výkone jeho funkcie.

Spolupráca medzi EÚ a *Organizáciou Severoatlantickej zmluvy*[5] (ďalej len „NATO" - North Atlantic Treaty Organization) sa na prvý pohľad môže javiť ako samozrejmosť, pretože okrem spoločných hodnôt je väčšina členov EÚ aj členmi NATO. Na rozdiel od NATO, ktorá je založená na kolektívnej obrane členských štátov, je záber EÚ širokospektrálny. EÚ sa zameriava nie len na obrannú zložku svojej *Spoločnej bezpečnostnej a obrannej politiky*[6] (ďalej len „SBOP"), ale aj na súvisiace oblasti ako je obranný priemysel a trh, obranný výskum a vývoj, s tým korešpondujúcu legislatívu a rôzne politické a finančné nástroje na jej podporu (Kolín, 2007, s. 88). Úspech vo vzájomnej spolupráci však nebol vždy stabilný a v niektorých rokoch dokonca výrazne absentoval. V súčasnosti, najmä v súvislosti s nárastom európskych bezpečnostných ambícií, ale aj rizík, obaja partneri vidia zásadné pridané hodnoty ich vzájomnej spolupráce pri budovaní spoločného partnerstva.

Cieľom príspevku je predstaviť vývoj budovania partnerstva EÚ a NATO, dotváranie ich vzájomnej spolupráce, tvorbu a obsah partnerských dohôd s ich následnou realizáciou v podobe spoločnej vojenskej kooperácie. Príspevok chronologicky popisuje významné medzníky tvorby SBOP ako dôsledok pre budovanie politickej a odbornej spolupráce EÚ a NATO s následnou jej realizáciou vo vojenskej spolupráci v záujmových regiónoch. Ilustruje skladbu vojenských riadiacich štruktúr ako kapacít velenia a riadenia EÚ, ich organizačné členenie a spôsobilosti, ktoré výrazným spôsobom ovplyvňujú vzájomnú vojenskú spoluprácu. Hlavným prínosom príspevku je objasnenie obsahu a významu jednotlivých rozhodujúcich vyhlásení a dohôd EÚ a NATO a načrtnutie obrazu novej stratégie európskej bezpečnosti a obrany. V závere príspevok prináša celkové zhrnutie uvedených faktov, na základe ktorých ponúka možnú víziu ďalšej cesty budovania partnerstva EÚ a NATO.

1. VÝVOJ VZŤAHOV EÚ A NATO

1.1 EURÓPSKA BEZPEČNOSTNÁ A OBRANNÁ POLITIKA

Jedným z najdôležitejších impulzov k začatiu jednania WEU o obrannej politike a vojenských kapacitách EÚ bol postoj premiéra Spojeného kráľovstva a francúzskeho prezidenta v decembri 1998 na ich spoločnom pracovnom stretnutí vo francúzskom Saint-Malo, ktorého výsledkom bola ich spoločná deklarácia. Tá obsahuje výzvu členským štátom WEU k založeniu spoločnej bezpečnostnej politiky WEU a vytvoreniu tomu odpovedajúcich vojenských štruktúr. Uvedená výzva bola potvrdená spoločnou deklaráciou na summite Európskej rady v rakúskej Viedni, ktorá pojednávala víziu rozvoja spoločnej obrany v Európe.

[5] Je medzivládna obranná vojenská organizácia s politickou kontrolou, založená 4. apríla 1949 podpisom tzv. Washingtonskej zmluvy ako reakcia západných demokratických štátov na vzniknutú povojnovú situáciu v Európe a eskaláciu napätia zo strany Sovietskeho zväzu.

[6] Je ako súčasť SZBP jedným z nástrojov uskutočňovania zahraničnej politiky EÚ.

Jej obsahom boli aj riešené otázky nových obranných kapacít WEU. Spoločná deklarácia nevytvárala požiadavky na kolektívnu obranu členských štátov EÚ, ale skôr sa zameriavala na plnenie Petersbergských úloh7 a úloh budovania potrebných vojenských a civilných kapacít WEU k splneniu týchto úloh rýchlou reakciou na vzniknuté krízové situácie.

Summit Európskej rady vo fínskych Helsinkách v roku 1999 v oblasti SZBP zostavil potrebný zoznam síl a prostriedkov pre sily rýchlej reakcie EÚ pod názvom Európsky základný cieľ (ďalej len „EHG" - European Headline Goal), ktorý navrhol vytvoriť vojenské kapacity EÚ do roku 2003 s kapacitou 15 brigád, čo je približne 60 000 osôb, spôsobilých k nasadeniu do 60 dní od prijatého rozhodnutia po dobu jedného roka v priestore operácií s akčným rádiusom 6000 km. Uvedené sily mali disponovať odpovedajúcou leteckou podporou, s kapacitou 500 bojových lietadiel, a námornou podporou, s kapacitou 15 bojových lodí. Ďalej v tejto zostave síl mali byť vytvorené dostatočné štruktúry logistickej podpory, prieskumu a prvkov velenia a riadenia. Časť týchto síl, ako predsunutá skupina, mala byť pripravená k nasadeniu do 48 hodín (Frank – Khol, 2003, s. 23). Tento zoznam bol niekoľkokrát revidovaný a bolo v ňom doplnené napríklad aj vytvorenie rezervy, tvorenej až z 5000 policajtov, ktorých určitá časť mala spôsobilosť k ich rýchlemu nasadeniu do priestoru operácií s pohotovosťou do 30 dní pre plnenie humanitárnych a záchranných misií, operácií na udržanie a nastolenie mieru (Fiala – Pitrová, 2003, s. 575). Myšlienka EHG ako spoločnej ambície tvorby vojenských kapacít EÚ sa však nestretla s pochopením členských štátov EÚ.

V roku 2000 sa Európska rada v portugalskom Santa Maria de Feira sa zaoberala novými štruktúrami európskej spoločnej obrany. Tento zámer bol definitívne schválený koncom roka 2000 na summite vo francúzskom Nice vydaním spoločného vyhlásenia o SBOP. Týmto vyhlásením bola potvrdená schopnosť vedenia vojenských misií a operácií EÚ krízového manažmentu so spôsobilosťami operačného plánovania NATO a poskytovania vojenských i nevojenských kapacít pre prevenciu medzinárodných konfliktov. V rámci tejto štruktúry bol zároveň ustanovený Politický a bezpečnostný výbor8 (ďalej len „PSC" - Political and Security Comitte), ktorého kompetencie majú zásadný význam aj v rámci budovania partnerstva medzi EÚ a NATO, a to formou spoločných rokovaní PSC a Severoatlantickej rady (ďalej len „NAC" - North Atlantic Council).

V ďalších rokoch SBOP posilňuje a konsoliduje spojenectvo EÚ so Spojenými štátmi americkými a Kanadou v rámci štruktúr NATO a súčasne rozvíja spôsobilosti brániť princípy Charty OSN. Príkladom obrany princípov Charty OSN je historicky prvá vojenská operácia EÚ (EUFOR ARTEMIS), ktorá bola vykonaná na základe rezolúcie Bezpečnostnej rady OSN v africkom Kongu v roku 2003. Tejto operácie sa zúčastnilo vyše 1400 osôb viacnárodného vojenského personálu. Operácia ARTEMIS ukázala, že členské štáty EÚ sú ochotné sa podieľať a prispieť k riešeniu krízovej situácie, a že EÚ má dostatočné schopnosti umožňujúce rýchlo reagovať (Kulíšek, 2007, s. 104).

V štruktúrach SBOP bola aj zároveň zakomponovaná stratégia financovania kapacít EÚ a to spôsobom, že finančné náklady na vedenie vojenských misií a operácií EÚ budú kryté z príspevkov členských štátov EÚ prostredníctvom finančného mechanizmu ATHENA9.

1.2 POLITICKÁ A ODBORNÁ SPOLUPRÁCA EÚ A NATO

[7] Predstavujú bezpečnostné, mierotvorné, humanitárne a úlohy v oblasti krízového manažmentu, ktoré si v roku 1992 stanovila WEU a ktoré prešli do agendy EÚ vďaka Amsterdamskej zmluve.

[8] Je výbor Európskej rady zodpovedný za SZBP a SBOP. Skladá sa z veľvyslancov členských štátov EÚ a predsedajú mu zástupcovia Európskej služby pre vonkajšiu činnosť.

[9] Prostredníctvom mechanizmu ATHENA sa môžu financovať spoločné náklady na vojenské operácie EÚ, ako aj náklady znášané štátmi, ako sú napr. náklady na ubytovanie, pohonné látky a podobné náklady súvisiace s národnými kontingentmi.

Akonáhle pominula bezpečnostná hrozba Sovietskeho zväzu, NATO začalo riešiť otázku ďalšieho uplatnenia v Európe. V novembri 1991 bola na summite NATO v talianskom Ríme prijatá strategická koncepcia. Naďalej definovala NATO ako obrannú organizáciu, ktorá považuje prítomnosť vojenských síl a prostriedkov Spojených štátov amerických v Európe za potrebnú a prínosnú (Fidler – Mareš, 1997, s. 217). NATO začalo uplatňovať svoj bojový potenciál ako partner rôznych organizácií v rámci vojenských operácií na podporu mieru v Európe. Zavedením SZOP sa začali Spojené štáty americké obávať možnej novej konkurenčnej bezpečnostnej organizácie v Európe. Na druhej strane, i keď neochotne sa vzdať vojenského vplyvu v Európe, presadili väčšiu vojenskú angažovanosť európskych štátov a zvýšenie ich podielu na financovanie vojenských misií a operácií NATO. Ako východisko sa stalo zriadenie Európskej bezpečnostnej a obrannej identity10, ktorá tvorila základ pre hľadanie cesty využívania operačných štruktúr a kapacít NATO. Jedna z hľadaných ciest bola aj navrhovaná koncepcia oddeliteľných avšak nie oddelených síl (Fiala – Pitrová, 2003, s. 588). Táto navrhnutá koncepcia Spojeným štátmi však bola na summite NATO v nemeckom Berlíne v roku 1996 odmietnutá. I napriek tomu tento summit z hľadiska vojenskej spolupráce medzi EÚ a NATO bol úspechom, pretože došlo k dohode o spolupráci medzi WEU a NATO. NATO sa rozhodlo sprístupniť pre WEU svoje spôsobilosti a kapacity za účelom plnenia úloh v rámci SZBP. Prijaté rozhodnutia sa stali základným pilierom pre vytvorenie Súboru dohôd označené ako "BERLÍN PLUS".

Na uvedenie tohto súboru do praxe museli obidve organizácie počkať, hlavne kvôli vetu Turecka ohľadom Cyperského problému11. Po troch rokoch vzájomných rozhovorov a riešenia kompromisov, Turecko nakoniec prestalo vetovať tento súbor dohôd. Avšak ku konečnému podpísaniu a schváleniu predchádzali dva dôležité kroky vzájomnej spolupráce. Prvým krokom bolo uzavretie dohody o bezpečnosti informácií, ktorá vytvorila mechanizmus výmeny utajovaných skutočností medzi obidvoma organizáciami a spoločné vyhlásenie EÚ a NATO o SBOP.

Na základe vzájomných rozhovorov PSC a NAC bol dopracovaný a schválený dňa 17. marca 2003 Súbor dohôd "BERLIN PLUS", ktorý poskytuje politickú a právnu základňu pre vojenskú spoluprácu EÚ a NATO v krízovom manažmente. Zároveň umožňuje, po vzájomnej spoločnej dohode, EÚ dostupnosť ku kapacitám12 a plánovacím spôsobilostiam NATO.

Následne na základe tohto súboru dohôd, NATO podporilo spôsobilosť riadenia vojenských operácií pod velením EÚ, odovzdaním svojej vojenskej operácie v Severnom Macedónsku (ALLIED HARMONY) v prospech vojenskej operácie (EÚ OPERATION CONCORDIA) a potom v roku 2004 prebehla transformácia a presun kompetencií na vojenskú operáciu v Bosne a Hercegovine (EUFOR ALTHEA) zo stabilizačnej operácie NATO (SFOR).

Inštitucionálnu vzájomnú spoluprácu zarámcovalo najmä spoločné vyhlásenie (Joint Declaration) z Varšavy v roku 2016, ktoré podpísali predseda Európskej rady, predseda Európskej komisie a generálny tajomník NATO, v ktorom obidve organizácie stanovili v deklarovanom „Súbore spoločných opatrení“ (Common Set of Proposals) prvých 42 opatrení, zo súčasných 74 opatrení, k budovaniu vzájomnej spolupráce na ďalšie obdobie. Spoločný

[10] Bola vypracovaná v rámci NATO s cieľom zvýšiť účasť Európy na otázkach bezpečnosti a zároveň posilniť transatlantickú spoluprácu. Neskôr bola nahradená SBOP.

[11] V roku 1998 začala južná časť ostrova Cyprus vyjednávať o vstupe do EÚ. Pokus dostať do EÚ celý ostrov, čiže aj Tureckú republiku severného Cypru, stroskotal v apríli tohto roka, keď grécki Cyperčania zamietli v referende zjednotenie ostrova.

[12] V tomto prípade zahŕňajú vojenské jednotky pre zabezpečenie velenia, vojenské štáby pre operácie krízového manažmentu a stále veliace štruktúry NATO.

súbor opatrení nie je samostatným dokumentom a musí sa vykladať v kontexte záverov Rady13 o vykonaní spoločného vyhlásenia. Stav začlenenia a transparentnosti opatrení, uplatňovanie paralelných postupov a akčných plánov je priebežne vyhodnocovaný formou „správ“ (Progress Report) zahrňujúce aj prípadné vylepšené a doplňujúce opatrenia na budúcu spoluprácu.

V ďalšom období na žiadosť Nemecka, Grécka a Turecka sa ministri obrany členských štátov NATO dohodli, že NATO sa spojí v medzinárodnom úsilím o zastavenie nezákonného obchodovania a nelegálnej migrácie v Egejskom mori a začne aktívne spolupracovať s Európskou agentúrou pre pohraničnú a pobrežnú stráž14 (FRONTEX). Tiež bolo rozhodnuté o podpore operácie EÚ SOPHIA v Strednom mori vyčlenením námorných, leteckých a logistických prostriedkov NATO a koordinácie zvyšovania situačného povedomia v danom regióne.

Prvá „správa“ v roku 2017 o plnení Súboru spoločných opatrení EÚ a NATO dospela k záveru, že obidve organizácie výrazne pokročili vo vzájomnej vojenskej spolupráci a to v boji proti hybridným hrozbám a väčšej súdržnosti v oblasti rozvoja spôsobilosti pri budovaní obranných kapacít partnerských štátov EÚ a NATO. Zároveň bola dopracovaná dohoda o zintenzívnení vzájomnej spolupráce prostredníctvom doplnenia ďalších vygenerovaných opatrení do Súboru spoločných opatrení, a to hlavne v oblasti vojenskej mobility, zdieľania informácií v boji proti terorizmu, posilnenia odolnosti voči rizikám súvisiacimi s chemickými, biologickými, rádiologickými a jadrovými rizikami a presadzovania bezpečnostného programu žien.

Vzhľadom k posledným aktuálnym udalostiam na Ukrajine, výrazne ovplyvňujúcim bezpečnosť Európy, sa EÚ a NATO zjednocujú v spoločnom vyhlásení odsudzujúce inváziu Ruskej Federácie na Ukrajinu, v politickej podpore ukrajinskej zvrchovanosti, jej územnej celistvosti a práva na sebaobranu. Spoločne a koordinovane začínajú procesy na vypracovanie novej globálnej stratégie na posilnenie bezpečnosti a obrany v Európe.

1.3 VOJENSKÁ SPOLUPRÁCA EÚ A NATO V ZÁUJMOVÝCH REGIÓNOCH

Okrem politickej a odbornej vzájomnej spolupráce na úrovni spoločných rokovaní a uzatváraní dohôd, paralelne prebiehala aj bezprostredná vojenská spolupráca priamo v rôznych krízových regiónoch v rámci strategického priestoru EÚ zobrazeného na obrázku číslo 1. Pre EÚ je kľúčová bezpečnostná stabilita svojho susedstva, ale aj regiónov podporujúce ekonomické a hospodárske aspekty rozvoja EÚ. Preto medzi prvými príkladmi tejto vzájomnej spolupráce bola koordinácia medzi misiou EÚ na podporu právneho štátu v Kosove (EULEX – The European Union Rule of Law Mission) a mierovými silami KFOR (Kosovo Force), zabezpečujúce naplňovanie rezolúcie Rady bezpečnosti OSN. Funkčnosť tohto procesu bola demonštrovaná v roku 2004 aj prepojením vojenskej operácie EÚ (EUFOR ALTHEA) v Bosne a Hercegovine, prevzatím úsilia od stabilizačných síl NATO (SFOR – Stabilisation Force). Zároveň boli poskytnuté kapacity Najvyššieho veliteľstva spojeneckých síl v Európe (ďalej len „SHAPE“- Supreme Headquarters Allied Powers Europe) v belgickom Monse pre operačné veliteľstvo EUFOR ALTHEA.

Potenciál budovania vzájomných vzťahov je aj v prepájaní vojenských spôsobilostí medzi NATO a EÚ v Indickom oceáne. Príkladom je odovzdávanie praktických odborných skúsenosti a koordinácia vojenskej námornej operácie NATO - OCEAN SHIELD a operácie

[13] Rada na základe usmernení, ktoré stanovuje Európska rada, vymedzuje a vykonáva SZBP. Patrí sem aj rozvojová a humanitárna pomoc, obrana a obchod EÚ. Spoločne s Vysokým predstaviteľom EÚ pre zahraničné veci a bezpečnostnú politiku zabezpečuje Rada jednotnosť, konzistentnosť a účinnosť vonkajšej činnosti EÚ.

[14] Agentúra EÚ založená v roku 2004 s cieľom pomáhať členským štátom EÚ a krajinám pridruženým k schengenskému priestoru pri ochrane vonkajších hraníc priestoru voľného pohybu EÚ.

EÚ - ATALANTA (EUNAVFOR SOMALIA), ktoré sa vykonávajú v boji proti pirátstvu a zabezpečovaní bezpečného prechodu námornej obchodnej prepravy v Adenskom zálive.

Výborné a nenahraditeľné skúsenosti vzájomnej spolupráce medzi NATO a EÚ boli aj v regióne Strednej Ázie a to konkrétne v Afganistane. Medzinárodné bezpečnostné a asistenčné sily pod vedením NATO (ISAF - International Security Assistance Force), ktoré v roku 2015 nahradila NATO vojenská operácia RESOLUTE SUPPORT, aktívne spolupracovali od roku 2016 s civilnou misiou EÚ na podporu právneho štátu (EUPOL – The European Union Police Mission in Afghanistan). EÚ sa tiež v Afganistane spolupodieľala pri financovaní civilných projektov v provinčných rekonštrukčných tímoch, ktoré riadilo NATO s niektorým členským štátom EÚ.

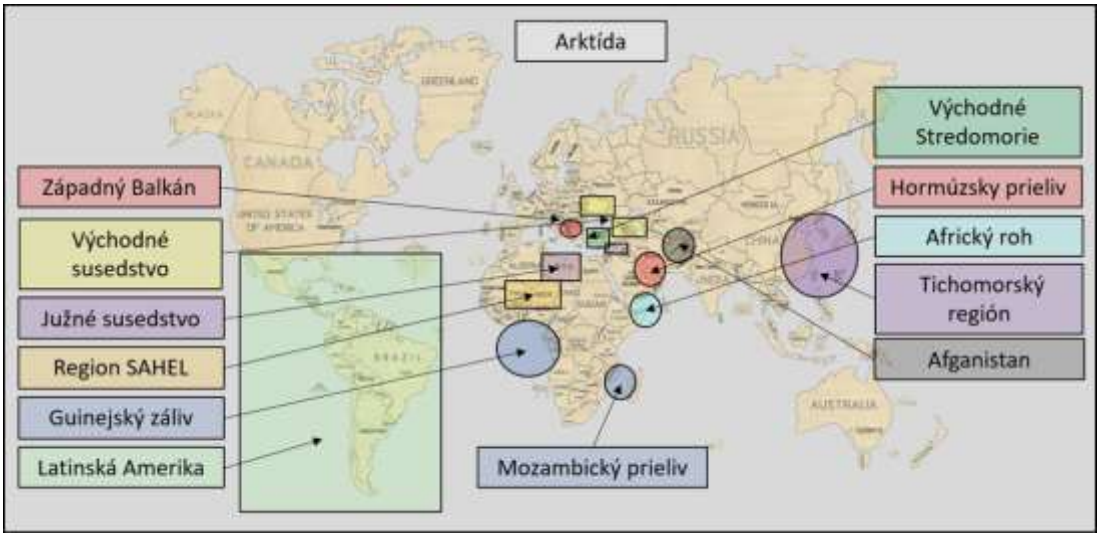
Podobný ráz má aj spolupráca EÚ a NATO v Iraku. Kým EÚ prostredníctvom poradnej civilnej misie (EUAM - European Union Advisory Mission) sa zameriava na rozvoj civilného bezpečnostného sektora, NATO pomáha prostredníctvom vlastnej vojenskej misie (NMI – NATO Mission Iraq) v budovaní kapacít irackých bezpečnostných a obranných štruktúr.

2. VOJENSKÉ RIADIACE ŠTRUKTÚRY EÚ

2.1 VOJENSKÝ VÝBOR EÚ

Vojenský výbor EÚ (ďalej len „EUMC“ - European Union Military Committee) bol zriadený rozhodnutím Európskej rady z 22. januára 2001. Je najvyšším vojenským orgánom v rámci Európskej rady a vedie všetky vojenské aktivity v rámci strategického priestoru EÚ, zobrazeného na obrázku 1, s dôrazom na plánovanie a vedenie vojenských misií a operácií v rámci SBOP a rozvoja vojenských spôsobilostí ozbrojených síl EÚ. V ďalšom poskytuje vojenské odborné poradenstvo PSC a odporúčania týkajúce sa vojenskej odbornej problematiky.

EUMC tvoria náčelníci generálnych štábov členských štátov EÚ, ktorých reprezentujú ich stáli vojenskí predstavitelia. Má stáleho predsedu, ktorý sa volí na zasadnutí výboru na úrovni náčelníkov generálnych štábov. Organizačná štruktúra EUMC a jeho funkčné postavenie je znázornené na obrázku 2.



Obrázok 1 Strategický priestor EÚ
Zdroj: Vlastné spracovanie

2.2 VOJENSKÝ ŠTÁB EÚ

Vojenský štáb EÚ (ďalej len „EUMS“ – European Union Military Staff) je od roku 2004 vojensko-odborný prvok v rámci Európskej služby pre vonkajšiu činnosť15. Poskytuje strategické vojenské a odborné poradenstvo Vysokému predstaviteľovi EÚ pre zahraničné veci a bezpečnostnú politiku prostredníctvom EUMC. Úlohou EUMS je poskytovať EUMC včasnú odbornú podporu a nepretržité hodnotenie situačného povedomia v strategickom priestore EÚ. EUMS vytvára a udržuje koncepciu strategického plánovania vojenských misií a operácií, využívania komunikačných a informačných systémov, potrieb vývoja vojenskej technológie a odborných školení k dosiahnutiu požadovaných spôsobilostí. Riadi vyčlenený vojenský potenciál v celom spektre aktivít v predchádzaní kríz, riadenia krízového manažmentu, podpory humanitárnej pomoci, reformy bezpečnostného sektoru, stabilizácie a evakuácie občanov EÚ. Na čele štábu EUMS je ustanovený Generálny riaditeľ (DGEUMS – Director General EUMS) a požadované spôsobilosti EUMS zabezpečuje približne 200 vojenských a civilných zamestnancov v organizačnej štruktúre zobrazenej na obrázku 2.

EÚ má v rámci svojich vojenských veliacich a riadiacich štruktúr dve možnosti využívania systému velenia a riadenia vojenských operácii, a to systém kombinovaného a autonómneho velenia a riadenia16. Pre systém autonómneho velenia a riadenia môžu byť podľa potreby využívané kapacity v štyroch určených operačných veliteľstvách (OHQ – Operation Headquarters). Jedná sa o kapacity aktivovaných operačných veliteľstiev ako napríklad v nemeckom Postupime, vo francúzskom Mont Valérien, v talianskom Ríme, v britskom Northwoode a v gréckej Larisse. Druhá možnosť spočíva vo využití kapacít NATO a to veliteľstva SHAPE, prostredníctvom styčného tímu EÚ pre NATO vyčleneného z organizačnej štruktúry štábu EUMS. Príkladom tejto možnosti velenia a riadenia je vedenie už spomínanej vojenskej operácie EUFOR ALTHEA v Bosne a Hercegovine. Od júna 2017 má EÚ tretiu možnosť využívania systému velenia a riadenia vojenských operácii prostredníctvom útvaru pre plánovanie a vedenie vojenských operácií priamo z Bruselu.

2.3 ÚTVAR PRE PLÁNOVANIE A VEDENIE VOJENSKÝCH OPERÁCIÍ EÚ

Útvar pre plánovanie a vedenie vojenských operácií EÚ (ďalej len „MPCC“ – Military Planning and Conduct Capability) predstavuje veľmi dôležitý organizačný prvok strategického autonómneho velenia a riadenia na posilnenie obrany a štruktúr krízového riadenia EÚ aj s cieľom vyhnúť sa zbytočnej duplicite s vojenskými aktivitami NATO. Tento útvar vznikol aj na základe dlhodobej absencie stálych veliacich štruktúr EÚ k podpore plánovania a vedenia vojenských operácií a misií EÚ, nakoľko EUMS na to nebol určený. MPCC pracuje pod politickou kontrolou a strategickým vedením PSC. Činnosť uvedeného útvaru prispieva k zefektívneniu vedenia európskych vojenských misií a k zlepšeniu výcviku vojenského personálu ozbrojených síl z členských štátov EÚ.

Má stálu organizačnú štruktúru velenia a riadenia na vojenskej strategickej úrovni zodpovednú za operačné plánovanie a vedenie neexekutívnych vojenských misií17 vrátane zostavenia, nasadenia, udržania a obnovy deklarovaných síl a prostriedkov členských štátov EÚ

---

[15] European External Action Service (EEAS) koordinuje vonkajšie činnosti EÚ. Ako diplomatická služba EÚ je tiež zodpovedná za vývoj a výkon spoločnej bezpečnostnej a obrannej politiky. Je riadená vysokým predstaviteľom EÚ pre zahraničné veci a bezpečnostnú politiku.

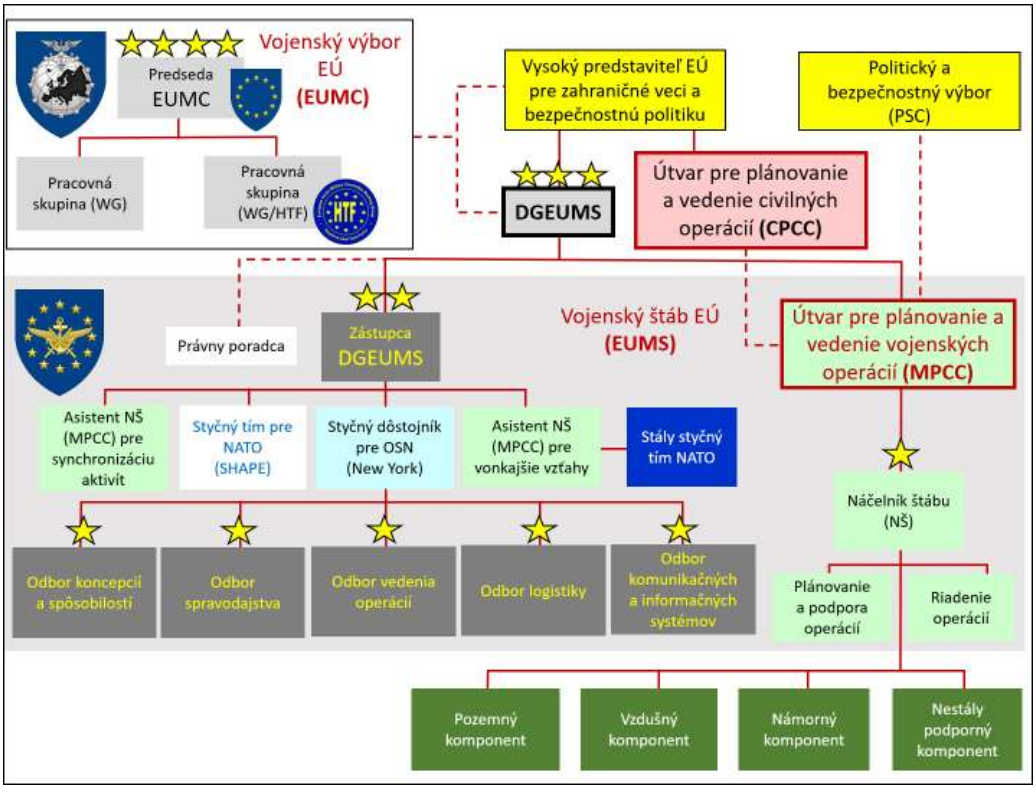
[16] Vojenská operácia EÚ je vedená bez použitia síl a prostriedkov NATO v súlade s koncepciou využívania spôsobilostí nosného členského štátu EÚ.

[17] Neexekutívna vojenská misia sa definuje ako vojenská operácia vykonávaná na podporu hostiteľskej krajiny, ktorá má len poradnú úlohu na rozdiel od výkonnej vojenskej operácie, ktorá je poverená vedením taktických a výcvikových aktivít v operačnom priestore hostiteľskej krajiny.

v operačnom priestore vojenskej misie. Zvyšuje schopnosť EÚ rýchlejšie a účinnejšie reagovať na vzniknuté ozbrojené konflikty alebo krízy vo svojom strategickom priestore, pričom ozbrojené sily EÚ sú nasadzované v úzkej koordinácii s ostatnými aktérmi SBOP v záujmovom regióne.

MPCC pozostáva približne z 25 stálych vojenských a civilných zamestnancov s možnosťou využívania podpory z iných odborov EUMS. Generálny riaditeľ štábu EUMS (DGEUMS) plní zároveň funkčné povinnosti veliteľa MPCC súvisiace s nasadzovaním a stiahnutím deklarovaných síl a prostriedkov členských štátov EÚ z vojenských misií, ako aj s celkovým rozpočtom, auditom a podávaním stanovených hlásení PSC a poskytovaním informácií EUMC.

V rámci posilnenia úzkej civilnej a vojenskej súčinnosti s cieľom zabezpečovať maximálnu koordináciu civilných a vojenských synergií a výmenu odborných vedomostí, útvar MPCC vzájomne spolupracuje s Útvarom pre plánovanie a vedenie civilných misií[18] prostredníctvom Spojeneckej podpornej koordinačnej skupiny[19]. Tento spôsob vzájomnej spolupráce vytvára schopnosť deliť sa o svoje praktické a teoretické skúsenosti, poznatky a najlepšie postupy v otázkach vedenia civilných misií, ako aj o spôsobilosti, keď budú civilné a vojenské misie nasadené súčasne v rovnakom operačnom priestore, vrátane lekárskej podpory alebo podpory iných ochranných opatrení.



Obrázok 2 Vojenská riadiaca štruktúra EÚ
Zdroj: Vlastné spracovanie

[18] CPCC - Civil Planning and Conduct Cabability. Útvar je určený ako operačný štáb pre civilné misie v rámci SBOP.
[19] JSCP – Joint Support Coordination Cell. Skupina je určená ku koordinácii civilných a vojenských odborných spôsobilostí na strategickej úrovni v rámci operačného plánovania a vedenia civilných misií EÚ.

Od konca roku 2020 je útvar MPCC spôsobilý vykonávať operačné plánovanie a vedenie výkonných vojenských operácií až do kapacity 2500 vojakov deklarovaných síl a prostriedkov členských štátov EÚ. MPCC v súčasnosti riadi tri vojenské výcvikové misie EÚ a to v africkom Mali (EUCAP MALI), v africkom Somálsku (EUCAP SOMALIA) a v Stredoafrickej republike (EUTM-RTC), ktoré sú zamerané na výcvik, podporu ozbrojených vládnych síl a posilňovanie vlád pri reforme bezpečnostného sektora uvedených afrických krajín.

3 VÝZNAMNÉ SPOLOČNÉ VYHLÁSENIA A DOHODY EÚ A NATO

3.1 SÚBOR DOHÔD „BERLIN PLUS“

Zasadanie NATO v severoamerickom Washingtone v roku 1999 dalo novú podobu mechanizmu BERLÍN20 za účelom jeho intenzívnejšieho a efektívnejšieho využitia. Súbor dohôd uzavreté medzi EÚ a NATO dostal pracovný nový názov „BERLIN PLUS“. Úplne presné a celkové znenie tohto súboru nie je verejnosti, vzhľadom k povahe stupňa utajenia v rámci NATO dostupné (KRAJCOVÁ, 2008, s.14). Preto obsah tohto súboru je prezentovaný zo všeobecných oficiálnych tlačových vystúpeniach z jednania EÚ a NATO.

Súbor dohôd obsahuje tri hlavné oblasti, ktoré sú priamo spojené s kombinovaným prístupom EÚ a NATO pri vedení vojenských operácií. Možnosť zaručeného prístupu vojenských riadiacich štruktúr EÚ ku kapacitám operačného plánovania NATO, k vopred vyčleneným kapacitám a spôsobilostiam NATO a využívaniu kapacít operačných veliteľstiev NATO pre velenie vojenským operáciám EÚ. Okrem iného zahŕňa aj funkčný rámec pre Zástupcu najvyššieho veliteľa spojeneckých síl v Európe (ďalej len „DSACEUR“ - Deputy Supreme Allied Commander Europe). Spojeným štátom sa nepodarilo presadiť v jeho funkčnej náplni úlohu koordinátora pre vojenské operácie EÚ, ktoré nevyužívajú kapacity NATO, avšak v rámci vojenských operácií, kedy EÚ využíva kapacity veliacich štruktúr NATO, funkcia koordinátora je plne akceptovaná dokonca s možnosťou veliteľa vojenskej operácie EÚ.

Spoločné vyhlásenie zo summitu v severoamerickom Washingtonu naviac spresňuje systém prispôsobenia plánu rozvoja spôsobilostí EÚ tak, aby bol schopný komplexnejšie a včasnejšie vyčleniť vhodné naplánované sily a prostriedky z obranného plánovania NATO, čím sa zabezpečí nepretržitá dostupnosť potrebných vojenských kapacít pre EÚ.

Do uvedeného spoločného vyhlásenia sa pripojujú ďalšie prvky ako napríklad dohoda o práci s utajovanými skutočnosťami, systémom konzultácií medzi obidvoma organizáciami, procedúrami zameranými na nasadzovanie, monitorovanie a stiahnutie vojenských síl a prostriedkov NATO. Je nutné však zdôrazniť, že žiadna oblasť a ani nie jej prvok sa nedá označiť pre vzájomnú spoluprácu medzi EÚ a NATO za najdôležitejší, pretože sú komplexne previazané.

Prístup k spôsobilostiam a kapacitám NATO je pre EÚ rozhodne dôležitý a prínosný. Avšak i napriek tomu sa EÚ môže bez nich za určitých podmienok neistoty a rizík obísť, využívaním dostupnosti národných vojenských spôsobilostí a kapacít členských štátov EÚ.

Neistota a riziko nezískania potrebného prístupu k spôsobilostiam a kapacitám NATO pramení aj z toho, že tento prístup je umožnený ako „predpokladaný“ a nie ako „zaručený“, čím podlieha schvaľovaciemu procesu Severoatlantickej rady, čo nie vždy môže byť vzhľadom na

[20] V roku 1996 sa stretla NAC v Berlíne a vyhlásila koncept Medzinárodných účelových zoskupení (CJTF – Combined Joint TaskForces), ktoré vytvárajú mechanizmus použití vojenských kapacít NATO pro WEU. Podľa záverov NAC z Berlína sa NATO rozhodlo, že dá svoje kapacity k dispozícii a že budú vytvorené konzultační mechanizmy medzi obidvoma organizáciami.

citlivosť reakčnej potreby vždy odsúhlasené (Krajcová, 2008, s.17). Jedná sa najmä o kapacity strategickej prepravy, mobilných prostriedkov velenia a riadenia a prostriedkov prieskumu.

Ak sa EÚ rozhodne pre svoju vojenskú operáciu využívať prístup ku kapacitám NATO na základe Súboru dohôd „BERLIN PLUS“, potom je garantovaný zo strany NATO, hlavne prístup k operačnému plánovaniu kapacitami veliteľstva SHAPE, ale aj inými kapacitami regionálnych operačných veliteľstiev NATO. Príkladom využitia iného regionálneho operačného veliteľstva bolo využitie veliteľstva NATO pre južnú časť Európy AFSOUTH (Allied Forces South) v talianskom Neapole pre vojenskú operáciu EU CONCORDIA.

V rámci systému konzultácií medzi EÚ a NATO, uvedený súbor dohôd umožňuje vytvorenie plánovacích prvkov v podobe spoločných styčných a koordinačných tímov dislokovaných priamo vo veliteľstve SHAPE alebo v štábe EUMS.

Súbor dohôd „BERLIN PLUS“ významným pokrokom a prínosom pre SBOP a to nie len ako teoretická platforma vzájomnej spolupráce, ale osvedčil sa aj v konkrétnych vojenských operáciách, ktoré jeho dohody a ustanovenia využili (Krajcová, 2008, s. 32).

3.2 SPOLOČNÝ SÚBOR OPATRENÍ TECHNICKEJ SPOLUPRÁCE MEDZI EÚ A NATO

Ďalším medzníkom rozvoja vojenskej spolupráce EÚ a NATO bolo vymedzenie vzájomnej technickej spolupráce formou prijatia Spoločného súboru opatrení ako súčasť spoločného vyhlásenia PSC a NAC z poľskej Varšavy. Od roku 2016 si EÚ aj NATO vyčlenili v Spoločnom súbore opatrení postupne až 74 opatrení. Prvé opatrenia boli zamerané na koordináciu pri reakciách na hybridné a kybernetické hrozby. V ďalšom sa pozornosť sústredila na vzájomnú spoluprácu pri obrannom, ale aj operačnom plánovaní tak, aby boli ich postupy a procesy vzájomne kompatibilné. Požiadavka bola aj zameraná na dosiahnutie kompatibility v oblasti vojenských spôsobilostí a to prostredníctvom vedenia vojenských taktických cvičení, ale už aj prebiehajúcich vojenských misií a operácií. Spoločný súbor opatrení je rozčlenený do siedmych strategických oblastí technickej spolupráce zobrazených na obrázku 3.

Obrázok 3 Strategické oblasti technickej spolupráce EÚ a NATO
Zdroj: Vlastné spracovanie

Hybridné hrozby

Prvá spoločná komplexná analýza hybridných hrozieb prebehla v novembri 2020 a mala značný význam najmä v snahe strategicky rozširovať vzájomnú spoluprácu. Aj preto bola v obidvoch organizáciách, ale aj európskych inštitúciách výrazne oceňovaná. Očakáva sa však, že EÚ a NATO by mohli do budúcna pokračovať okrem analýz aj s dohodami o spoločnom a jednotnom posudzovaní hrozieb. Z deklarovaných hrozieb, ktorým obidve organizácie venujú spoločne najviac pozornosti, sú kybernetické a hybridné útoky. Veľkú pridanú hodnotu v tejto oblasti prinieslo poznanie, podľa ktorého sa môže známy článok 521 Severoatlantickej zmluvy zo dňa 4 apríla 1949, teda že útok na jedného člena NATO znamená útok na všetkých členov NATO, uplatniť aj v prípade hybridnej vojny. Dôkaz, že táto strategická oblasť technickej spolupráce je hodnotená s vysokou dôležitosťou je, že už len zo 74 spoločných opatrení sa 20 opatrení týka práve tejto oblasti ako napríklad opatrenia na boj proti dezinformáciám, spolupráce v oblasti zvyšovania odolnosti, rozvoja civilnej obrany, schopnosti poskytovania prvej pomoci, úsilia v boji proti terorizmu a v posilnení odolnosti voči rizikám súvisiacimi s chemickými, biologickými, rádiologickými a jadrovými rizikami.

Európske centrum pre boj proti hybridným hrozbám (Hybrid CoE - European Centre of Excellence for Countering Hybrid Threats) vo fínskych Helsinkách úzko spolupracuje s ostatnými centrami výnimočnosti NATO pre boj proti hybridným hrozbám ako napríklad Centrom pre strategickú komunikáciu (Strategic Communications Centre of Excellence) v lotyšskej Rige, Centrom výnimočnosti NATO kybernetickej bezpečnosti (Cooperative Cyber Defence Centre of Excellence) v estónskom Taline a Centrom výnimočnosti NATO pre energetickú bezpečnosť (Energy Security Centre of Excellence) v litovskom Viľnuse.

Kybernetická bezpečnosť

V rámci EÚ pôsobí Agentúra EÚ pre kybernetickú bezpečnosť 22 (ENISA - European Union Agency for Cyber security), ktorá úzko spolupracuje v oblasti kybernetickej obrany s Centrom výnimočnosti NATO pre koordináciu kybernetickej bezpečnosti (Cooperative Cyber Defence Centre of Excellence) dislokovanom v estónskom Taline. Práve takáto vzájomná spolupráca a odbornejšia koordinácia týchto dvoch nástrojov sa považuje za veľmi dôležitý spôsob spoločnej reakcie na zvyšujúci sa počet, ale aj kreativitu spôsobu vykonávania kybernetických útokov. Stále však chýba návod, akým spôsobom nájsť pôvodcov a vinníkov, ale aj ako reagovať koordinovane, a najmä rýchlo. Z tohto dôvodu sa vytvára myšlienka na vytvorenie spoločného informačného uzla pre kybernetické hrozby, či spoločnej osobitnej skupiny EÚ a NATO pre kybernetickú bezpečnosť aj v podobe súčinnosti medzi už existujúci Tímom reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU – Computer Emergency Response Team) a inštitúciou Nástrojom NATO pre reakciu na počítačové incidenty (NCIRC – NATO Computer Incident Response Capability).

---

[21] Zmluvné strany sa dohodli, že ozbrojený útok proti jednej alebo viacerým z nich v Európe alebo Severnej Amerike sa bude považovať za útok proti všetkým, a preto odsúhlasili, že ak nastane taký ozbrojený útok, každá z nich uplatní právo na individuálnu alebo kolektívnu obranu uznané článkom 51 Charty Spojených národov, pomôže zmluvnej strane alebo zmluvným stranám takto napadnutým tým, že bezodkladne podnikne sama a v súlade s ostatnými stranami takú akciu, akú bude považovať za potrebnú, vrátane použitia ozbrojenej sily s cieľom obnoviť a udržať bezpečnosť v severoatlantickej oblasti.

[22] Agentúra ENISA zohrávala úlohu pri koncepcii kybernetickej bezpečnosti EÚ, ktorá predstavuje odporúčanie členským štátom EÚ, aby koordinovane reagovali na rozsiahle cezhraničné kybernetické incidenty a krízy na úrovni EÚ.

Operačná koordinácia

Táto oblasť je zameraná najmä na koordináciu námorných vojenských aktivít v uplatňovaní vzájomne dohodnutého mechanizmu Spoločného informovania a riešenia konfliktov v Stredozemnom mori SHADE MED (Shared Awareness and Deconfliction in the Mediterranean), v rámci ktorého EÚ a NATO zdieľajú praktické skúsenosti v oblasti koordinácie námorných aktivít v operáciách námorných síl EÚ vo vojenskej operácii SOPHIA a námornými silami NATO vo vojenskej operácii SEA GUARDIAN. V súčasnosti v Stredozemnom mori bola spustená nová námorná vojenská operácia EÚ IRINI, ktorá je zameraná na presadzovanie zbrojného embarga voči africkej Líbyi.

Oblasť operačnej koordinácie spresňuje aj iné formy odovzdávania skúseností ako je napríklad organizovanie odborných seminárov zameraných na diskusie o skúsenostiach námorných vojenských operácií obidvoch organizácií v boji proti pirátstvu v Indickom oceáne. Operačná koordinácia nie je len zameraná na námorné vojenské aktivity, ale aj vzájomnú spoluprácu vojenských štábov EÚ a NATO v rámci vzdušných operácií Západného Balkánu (BANM – Balkans Normalisation Meetings).

Priemysel a výskum

Oblasť technologického a priemyselného partnerstva pokrýva transatlantická obranná, technologická a priemyselná spolupráca. V jej rámci chce NATO spoločne s Európskou obrannou agentúrou23 (EDA – European Defence Agency) uľahčiť transatlantický technologický a priemyselný rozvoj. Aj tu však panujú nedostatky. Nedoriešené oblasti, v ktorých vidia mnohí potenciál na bližšie prepojenie, sa týkajú bezpečnosti dodávok, spoločného prístupu k právam duševného vlastníctva, priamym zahraničným investíciám, či recipročnému prístupu na trhy v oblasti obranných zariadení. Práve reciprocita je témou, ktorá v kontexte rozširovania európskych snáh o strategickú autonómiu trápi členov NATO, ktorí nie sú členmi EÚ. Doteraz bolo totiž otázne, či dostanú možnosť participovať na európskych projektoch PESCO24, v rámci ktorých EÚ vyvíja nové obranné spôsobilosti a technológie. Nakoniec bolo rozhodnuté Radou, že prístup tretích krajín bude možný za špecifických okolností v strategickom záujme EÚ i napriek tomu, že väčšina PESCO projektov je dnes v súlade s prioritami obranného plánovania NATO. Prvým konkrétnym príkladom bolo rozhodnutie Rady z mája 2021, ktorým bolo povolené koordinátorovi projektu vojenskej mobility, teda Holandsku, prizvať Spojené štáty a Kanadu na základe ich žiadostí k účasti na tomto projekte.

V súvislosti s rapídnym rozvojom technológií, ktoré sa dostávajú aj do obranného priemyslu, narastá aj význam kozmického priestoru. NATO sa tejto oblasti venuje o čosi intenzívnejšie, a to aj vďaka aktivitám Spojených štátov, ktoré patria v tejto oblasti medzi celosvetových lídrov. EÚ rovnako prevádzkuje programy ako GALILEO25, COPERNICUS26,

---

[23] Agentúra ktorá podporuje členské štáty a Radu v ich úsilí o zlepšenie európskeho obranného potenciálu v oblasti krízového riadenia a podporuje politiku Európskej bezpečnostnej a obrannej politiky (ESDP) v súčasnosti a v rámci budúceho vývoja.

[24] Stála štruktúrovaná spolupráca (PESCO – Permanent Structured Cooperation), predstavuje nástroj na posilnenie spolupráce v oblastiach budovania obranných a vojenských spôsobilostí, výšky investičných výdavkov v oblasti obrany vrátane výskumu a vývoja, posilnenia dostupnosti a schopnosti nasadenia ozbrojených síl zúčastnených členských štátov EÚ.

[25] GALILEO je navigačný kozmický systém realizovaný EÚ na určovanie polohy a navigácie na Zemi.

[26] COPERNICUS je vesmírny program financovaný EÚ zameraný na diaľkový prieskum Zeme na pozorovanie jej atmosféry, pevniny, morí a klímy.

alebo Satelitné stredisko EÚ (SatCen) v španielskom Torrejón de Ardoz, avšak zatiaľ iba v civilnej sfére.

Obranné spôsobilosti

V tejto strategickej oblasti je hlavný dôraz položený na ucelenosť výstupov medzi procesom obranného plánovania NATO (NDPP - NATO Defence Plannig Process) a plánom rozvoja spôsobilostí EÚ prostredníctvom účasti vojenských štábov EÚ a NATO na pracovných stretnutiach v rámci obranného plánovania NATO. Vzájomná komunikácia na pracovných stretnutiach vytvorí vecnosť a účelovosť pri tvorbe investícia spoločného rozvoja obrany. Na základe týchto poznatkov sa pravidelne aktualizuje zoznam projektov, ktoré sa realizujú v rámci PESCO. Od decembra 2016 sa do zoznamu existujúcich 46 projektov pridávajú ďalšie a ďalšie projekty v rámci dôležitosti a kritických nedostatkov kapacít. Medzi také projekty sú zaradené napríklad projekt strategickej leteckej prepravy nadmerného nákladu, projekt vývoja novej generácie taktických bezpilotných vzdušných prostriedkov, projekt kybernetickej obrany systémov velenia a riadenia a tak ďalej. Zoznam nových projektov zahŕňa aj vývoj európskych sprievodných plavidiel pre námorníctvo, budúcich taktických nákladných vozidiel strednej veľkosti, tankovacie lietadlá, ručné zbrane s meniteľnou veľkosťou. K vývoju a vojskovým skúškam sú z PESCO projektov aj financované vývojové zariadenia ako napríklad Simulačné a skúšobné centrum pre bojové tanky (MBT – SIMTEC Main Battle Tank Simulation and Testing Center) určené hlavne pre vývoj a vojskové skúšky prostriedkov pozemných vojenských operácií.

Budovanie kapacít

Vojenské štáby EÚ a NATO v rámci tejto oblasti zintenzívnili odbornú spoluprácu zameranú na budovanie kapacít a odolnosti, najmä v Západnom Balkáne a vo Východnom a Južnom susedstve vrátane Gruzínska, Moldavskej republiky, Ukrajiny, Jordánska, Maroka a Tuniska. Budovanie kapacít a odolnosti v uvedených regiónoch je zamerané hlavne na efektívnu podporu činnosti spravodajských služieb, strategickej komunikácie27 (STRATCOM – Strategic Communication), kybernetickej obrany a boja proti terorizmu. Zvyšovanie odbornej spolupráce je zabezpečované výmenou odborných znalostí prostredníctvom centier výnimočnosti (CoE) a iných príslušných vzdelávacích činností a programov.

V rámci budovania kapacít sú neustále analyzované a identifikované aktuálne schopnosti a možnosti účasti členských štátov EÚ a NATO na vzájomných projektoch a praktických programoch partnerstva s prioritou budovania vojenských námorných kapacít.

Vojenské cvičenia

V rámci pilotného projektu tejto strategickej oblasti na roky 2017 a 2018 sa uskutočňovali paralelné a koordinované vojenské cvičenia EÚ a NATO. NATO bolo určené ako riadiaci v rámci vojenského cvičenia krízového riadenia v roku 2017 (CMX - Crisis Management Exercise) a EÚ riadiacim v rámci vojenského cvičenia viacúrovňového krízového riadenia v roku 2018 (ML - Multi-Layer Crisis Management Exercise). Bolo dohodnuté, že v rámci tvorby scenárov vojenských cvičení je potrebné vždy zakomponovať udalosti týkajúce sa minimálne jedného prvku hybridného útoku.

[27] Systematické a koordinované používanie objektívnych informácií verbálnymi a neverbálnymi spôsobmi komunikácie s cieľom napĺňať strategické záujmy štátu.

Na základe aktuálnych podmienok a vývoja bezpečnostnej situácie je potrebné vždy flexibilne reagovať prijatím vhodných foriem a metód vojenských cvičení, tak ako to bolo počas vojenských cvičení NATO CMX 20 (STEAD FAST JUPITER/JACKAL), kedy vplyvom plnenia opatrení proti COVID 19 uvedené vojenské cvičenia prebiehali v on-line režime.

Vybraný vojenský personál vojenských štábov EÚ alebo NATO, ktorých organizácia nebude v danom roku riadiacim vojenského cvičenia, je vyzvaný, aby v rámci reciprocity participoval pri tvorbe a realizovaní plánu vykonania vojenského cvičenia.

Je potrebné v čo najväčšej miere si vymieňať skúsenosti a odporúčania identifikované v záverečných rozboroch vojenských cvičení k doladeniu alebo k zmene stálych operačných postupov pri taktických aktivitách vojenských jednotiek alebo procesoch vojenských štábov. Na základe odporúčaní (LL – Lessons Learned) je nevyhnutné podporovať vojenské odborné vzdelávania vzájomným pozývaním odborníkov na podujatia ako sú semináre, prezentácie alebo samotné vojenské cvičenia.

3.3 NOVÁ STRATÉGIA EURÓPSKEJ BEZPEČNOSTI A OBRANY

V súčasnosti EÚ aj NATO začali proces reflexie s cieľom náležite sa prispôsobiť bezprecedentným globálnym zmenám a novým výzvam v oblasti bezpečnosti a obrany. Pandémia ochorenia COVID-19 má výrazný vplyv na medzinárodné vzťahy, ale hlavne na národné rozpočty a spôsobila ďalšie zhoršenie existujúceho globálneho napätia a nových bezpečnostných výziev. EÚ a NATO od začiatku pandémie úzko spolupracovali a riešili otázky, ako sú distribúcia zdravotníckeho materiálu a pomôcok, výstavba a rozmiestňovanie poľných nemocníc, dostupnosť zdravotníckeho personálu, ale aj nárast prípadov kybernetických útokov, špionáže štátnych a neštátnych subjektov proti členským štátom EÚ a spojencom NATO v súvislosti s pandémiou ochorenia COVID-19. Na základe týchto skúseností je zdôraznená skutočnosť, že európske úsilie v oblasti odolnosti musí ako základ zahŕňať aj jasnú verejnú komunikačnú stratégiu k zvýšeniu informovanosti verejnosti o európskych a transatlantických bezpečnostných výzvach.

Vrcholný predstavitelia členských štátov EÚ sa v júni 2020 dohodli na začatí procesu nových bezpečnostných vízii vymedzených v Strategickom kompase EÚ a Globálnej stratégie zahraničnej a bezpečnostnej politiky EÚ. Tento proces tvorby bol spustený ako nutná potreba súbežného procesu tvorby novej Strategickej koncepcie NATO do roku 2030. Prebiehajúce procesy tvorby a realizácie novej stratégie bezpečnosti a obrany v Európe ponúkajú jedinečnú príležitosť na ďalšie zintenzívnenie vzájomných konzultácií a spolupráce s cieľom posilniť bezpečnosť Európy a podporiť mier a stabilitu. Spoločná vízia zdôrazňuje výzvu, aby sa súbežne uskutočňovali prebiehajúce, ale aj budúce práce na doplňovaní Strategického kompasu EÚ a Strategickej koncepcie NATO, s cieľom vždy stanovovať jasné priority a určovať dodatočné synergie v záujme posilnenia transatlantickej väzby a ďalšej spolupráce s členskými štátmi EÚ. Integrovaným prístupom v spoločnej stratégii EÚ a NATO pri určovaní a analýzach hrozieb sa náležite bude zohľadňovať dlhodobý bezpečnostný rozmer krajín v bezprostrednom susedstve EÚ, najmä Východného susedstva a Západného Balkánu.

Okrem regiónov susedstva EÚ narastá obrovský strategický význam regiónov ďalekého severu a Arktídy a ich politický, hospodársky, environmentálny a bezpečnostný rozmer udáva význam koordinácie medzi EÚ a NATO v Arktíde. Arktída musí zostať oblasťou mierovej spolupráce, preto sa požadujú opatrenia na budovanie dôvery, aby sa zabránilo krokom vedúcim k navýšeniu vojenskej prítomnosti akéhokoľvek štátu v tomto regióne. EÚ v súčasnosti aktualizuje svoju politiku pre Arktídu a opakuje svoju výzvu na posilnenie spolupráce so všetkými arktickými partnermi, a to na bilaterálnej, ale aj regionálnej úrovni.

ZÁVER

Zhrnutím poznatkov z príspevku je možné konštatovať, že počiatkom významných medzníkov budovania partnerských vzťahov vo vojenskej spolupráci medzi EÚ a NATO bola myšlienka EHG ako impulzu tvorby vojenských kapacít EÚ. Táto myšlienka sa však stretla s nevôľou zo strany členských štátov EÚ. Dôvodom boli deklarované nedostatočné vojenské kapacity členských štátov EÚ a tento cieľ sa nepodarilo prakticky realizovať. Napriek tomu tento neúspech nasmeroval úsilie EÚ v rámci SBOP na vzájomnú vojenskú spoluprácu s NATO s víziou obojstrannej podpory a koordinácie pri dosahovaní spoločných cieľov. Správne nasmerovanie úsilia EÚ potvrdzuje ďalší významný medzník v podobe deklarácie Súboru dohôd „BERLIN PLUS“, ktorého obsah vytvára potrebné podmienky vojenským riadiacim štruktúram EÚ k využívaniu kapacít veliacich štruktúr NATO. Súčasťou tohto súboru dohôd sú aj určené opatrenia vzájomnej koordinovanej spolupráce počas vojenských operácií a misií v záujmových regiónoch. Vymedzenie Spoločného súboru opatrení v definovaných strategických oblastiach, bol ďalším medzníkom rozvoja vzájomných vzťahov obidvoch organizácií. Dôraz tohto súboru opatrení bol síce položený na technickú spoluprácu, ale tento spôsob spolupráce vytvoril lepšie podmienky vzájomnej previazanosti a efektívnejšieho vnímania potrieb k dosahovaniu spoločných cieľov.

Nový vietor do plachiet spoločného partnerstva prinieslo v súčasnom období viacero faktorov. Vo vhodnom čase sa totiž stretol záujem na oboch stranách Atlantiku. Kým Spojené štáty v minulom prezidentskom období odvracali pozornosť od medzinárodných partnerstiev, EÚ si v tom čase začala zásadnejšie uvedomovať svoju bezpečnostnú a obrannú závislosť na Spojených štátoch. To podnietilo aj otvorenosť viacerých európskych štátov, na čele s Francúzskom a Nemeckom, aktualizovať európsku bezpečnostnú a obrannú spoluprácu. Kým EÚ zistila, ako nákladné a technologicky náročné bude prebrať zodpovednosť obranných spôsobilostí v Európe, v Spojených štátoch nastalo nové prezidentské obdobie s novým prezidentom Spojených štátov, ktorý hneď v úvode svojho mandátu vyjadril jasný zámer spolupracovať s partnermi v EÚ a NATO vo všetkých strategických oblastiach technickej a vojenskej spolupráce. Ucelený rozvoj spôsobilostí členských štátov EÚ prostredníctvom Súboru spoločných opatrení v rámci technickej spolupráce medzi EÚ a NATO prispeje k posilneniu potrebných spôsobilostí, ktoré sú potenciálne k dispozícii obom organizáciám i napriek tomu, že sa uvádza ich odlišná povaha a zodpovednosť. EÚ opätovne potvrdzuje, že vzájomná spolupráca bude naďalej prebiehať v duchu úplnej otvorenosti a transparentnosti, pri plnom vzájomnom sa rešpektovaní pri tvorbe, ale i uplatňovaní novej stratégie na ďalšie obdobie. Súčasná tvorba globálnej stratégie bezpečnosti a obrany z pohľadu EÚ a NATO má každopádne spoločný prienik v otázkach budovania kapacít, rozvoja technológií, posilnenia odolnosti vo vzťahu k hybridným hrozbám, ale hlavne k pochopeniu, že úspešnosť novej stratégie je hlavne vo vzájomnej a koordinovanej komunikácii s regionálnymi partnermi.

Jedinečnosť ďalšej spolupráce EÚ a NATO bola dosiahnutá po odchode Spojeného kráľovstva z EÚ. NATO je totiž naďalej jedinečným fórom pre bilaterálnu spoluprácu v oblasti bezpečnosti a obrany medzi EÚ a jej bývalým členským štátom, Spojeným kráľovstvom.

EÚ má v súčasnosti v reakcii na krízu oveľa bližšie ako mala v 90 rokoch minulého storočia, ale je stále ešte ďaleko od schopnosti efektívne a rýchlo autonómne generovať deklarované sily a prostriedky členských štátov EÚ, nasadiť ich a z jedného miesta velenia veliť vojenským operáciám, nehovoriac o neochote stálej pripravenosti členských štátov EÚ potrebné kapacity poskytnúť a financovať ich nasadenie (Kolín, 2020, s. 116). Z tohto dôvodu, ale aj vzhľadom k zhoršeniu aktuálnej bezpečnostnej situácii v Európe, je naopak možné očakávať obojstrannú snahu o zintenzívnenie budovania vzťahov medzi EÚ a NATO, čím sa zefektívni pripravenosť k nasadeniu síl a prostriedkov obidvoch organizácií. Ako poznamenal

prvý americký prezident George Washington v čase americkej vojny za nezávislosť „Byť pripravený na vojnu je jedným z najúčinnejších spôsobov zachovania mieru“.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

An Alliance in the 21st Century. 1999. [online]. Dostupné na internete: http://www.nato.int/docu/pr/1999/p99- 064e.htm.

EUFOR Mission. 2022. [online]. Dostupné na internete: http://www.euforbih.org/eufor/index.php?option=com_content&task=view&id=12&Itemid=28.

Evropská unie a NATO. 2006. [online]. Dostupné na internete: http://www.euractiv.cz/bezpecnost-a-spravedlnost0/linkdossier/evropsk-unie-a-nato.

DE WITTE, P. 2003. *Pokrok ve vztazích EU-NATO*. [online]. Dostupné na internete: http://www.nato.int/docu/review/2003/issue3/czech/art2.html.

FIALA, P., PITROVÁ, M. 2003. Evropská unie, Brno: Centrum pro studium demokracie a kultury, 2003.670 s. ISBN 9788073250157.

FIDLER, J., MAREŠ, P. 1997. Dějiny NATO, Praha: Paseka, 1997. 243 s. ISBN 80-7185-145.

FRANK, L., KHOL, R. 2003. Evropské bezpečnostní struktury. In *Obrana a strategie*. Univerzita obrany Brno. ISSN 1802-7199, 2003.roč.2003. č. 2.s. 17-26.

HARVÁNKOVÁ, V. 2016. *Vývoj spoločnej zahraničnej a bezpečnostnej politiky Európskej únie po Lisabonskej zmluve:* Bakalárska práca. Brno: Mendelova univerzita v Brně Fakulta regionálního rozvoje a medzinárodních studií. 47 s.

KOLÍN, V. 2020. Spoločná bezpečnostná a obranná politika EÚ v kocke – časť prvá. In *Vojenské rozhledy.* Ministerstvo obrany Českej republiky. Praha. ISSN 1210-3292, 2020.roč. XXIX. č. 4/2020. s. 87-101.

KRAJCOVÁ, J. 2008. *Berlín plus a Evropská bezpečnostní a obranná politika:* Bakalárska práca. Brno: Masarykova univerzita fakulta sociálních studií. 40 s.

KULÍŠEK, J. 2007. Operace Artemis (Model vytváření operačních svazků Battle Groups). In *Vojenské rozhledy*. Univerzita obrany Brno. ISSN 1210-3292,2007. roč. 2007. č. 2. s. 95-105.

PALÁN, V. 2003. *Společné cvičení EU a NATO v krizovém řízení*. [online]. Dostupné na internete: http://www.army.cz/scripts/detail.php?id=3134.

PROCHÁZKA, J. 2006. *Mise EU a Bojová uskupení EU: významný nástroj realizace bezpečnostní politiky EU*. [online]. Dostupné na internete: http://www.eurobb.cz/CZ/informacni-texty/mise-abojova-uskupeni-eu.html.

ROBERTSON, G. 2003. *Berlin plus, NATO and the EU*. [online]. Dostupné na internete: http://www.paginedidifesa.it/2003/natosg_031022.html.

The NATO-EU Strategic Partnership. 2004. [online]. Dostupné na internete: http://www.nato.int/docu/comm/2004/06-istanbul/press-kit/006.pdf.

ZÁVĚŠICKÝ, J. 2004. *ESDP a deficit vojenských kapacit evropských spojenců*. [online]. Dostupné na internete: http://www.globalpolitics.cz/clanek/esdp.html.

Ing. Ivan BYSTRIANSKY
Externý doktorand Katedry bezpečnosti a obrany
Akadémia ozbrojených síl gen. M. R. Štefánika
Demänová 393, 03101 Liptovský Mikuláš
bystriansky18@gmail.com

EASTERN EUROPE REFLECTED BY THE COPENHAGEN SCHOOL OF SECURITY

Anna ĎURFINA

ABSTRACT

The Copenhagen School, as one of the most fundamental security concepts, has brought new insights into global security, i.e. by introducing the regional security complex theory. This cornerstone of security analysis enables thus to analyze all regions globally and predict and explain developments in a particular region. The mail goal of the paper is to study main determinants of the Russian federation's influence on the regional security complex (hereinafter referred to as RSC or Complex) around its territory, and is based on verifying these main hypotheses and consequently, to verify the hypothesis that a separate Eastern RSC is likely to develop in nearest future. The second hypothesis on ratio of powers in RSC around Russia is influenced by the power in its centre (i.e. by the Russia's one covering also the Eastern Europe) is proved, too. The third hypothesis analyzed here was also confirmed claiming that the border of the RSC around Russia has shifted simultaneously as the buffer zone of the RSC's central power shifted. Therefore, the research needs to include past-given current developments in Eastern Europe. The methodology used in researching this issue is based on the methods of analysis and synthesis, the logical-historical method and the method of deductive approach. The study presented in this paper is built also on a long-time previous research on RSC around Russia. Concluding prediction of eventual Eastern regional security complex subsuming the RSC around Russia must be left to further academic and scientific discussion.

Keywords: Russian Federation, Eastern Europe, Copenhagen school of security, Regional Security Complex

INTRODUCTION

The regional security complex around Russia is a complex that evolved on the historical premise of one of the powers that was in the past and nowadays has been a basic element of the geopolitics of the space in question. The Soviet Union and the Russian Federation today have a significant impact on the adjoining region, in line with its territorial and military potential.

The answer to the question of how it shapes and then influences the regional security complex around Russia, as defined by Buzan and Wæver in their work *Regions and Powers* (2006), is important from the point of view of setting the security strategies of the individual countries that are currently at the borders with this power, as well as in the buffer zone of the Russian Federation. The construction of the security system in thus directly proportional to the definition of the regional security complex (RSC) created in the part of Eastern Europe under examination. If we have defined the necessity of analyzing the selected region through each country that is located in the region and based on the relationships that exist in that part of the world, the importance of choosing a correct theory of security is unquestionable.

In this connection, the basic hypotheses in this article will be based on the application of the basic principles of the security theory of the Copenhagen School, which by its premises allows exploration of the creation of security complexes in the world. Buzan's concept of security complex offers an appropriate analytical tool for the study of regional security complex around Russia and for the study of Russia's position in this region. The concept also

provides a conceptual framework for a more objective analysis of the current situation in Eastern Europe and more realistic prediction of its (regional security complex around Russia) probable future development based on the discovery of the major trend in this region.

Therefore, according to mail goal, the main hypothesis represents the thesis that the regional security complex around Russia was/is variable in time and space, ratio of powers in this RSC is influenced by the power in its centre and the border of the RSC around Russia has shifted in direct line to the shift of the buffer zone of the central power of the complex.

1 REGIONAL SECURITY COMPLEX AROUND RUSSIA IN LITERATURE

Buzan and Wæver (2006) represent such model of regional security that enables to analyze, and even anticipate and explain, developments within any region.

Hofreiter (2016) states that each regional security complex, even regional security complex around Russia can be described at for levels:

1. Level of complex units: level of safety and security situation in each unit - state complex.
2. Regional level: relations between the units that shape the nature of the security complex.
3. Trans-regional level: relations between neighboring regional security complexes.
4. Global level: the impact of global actors, including global powers, on regional security complexes.

Depending on the nature of the changes in the security complex structure, their effects may be according to Buzan et al. (2005) and Hofreiter (2016) as follows:

- Maintaining the status quo, so the regional complex remains unchanged - neither hostility, friendship or the distribution of power change.
- The regional complex transforms on internal level structure without change of the external boundaries of the complex. There is change in relationship of friendship and hostility, or creating closer links between units.
- The regional complex transforms on external level when some units are integrated from the security complex or external units are drawn into the security complex.
- Regional security complex is overlapped with one or more external powers, thereby suppressing the local character of security relations within the complex.

As Buzan and Wæver (2006) write, in the early years after the Cold War official end, Europe faced the decision create one, two, or even three regional security complexes. Finally, two regional security complexes in Europe were created. The geographic proximity of two powers (European Union and the Russian Federation) opens the theory a possibility to interlink two complexes, while in the 1990s even experts considered the formation of “free super-complex”.

According to Christensen (2002), in the post-Cold War time, Russia failed to construct a future self-perception and vision some attractive role and form. Shift in foreign policy was closely linked to the domestic sparse opposition against liberal reformers. Both Communists and nationalists gained more solid ground and the President did de facto accept a lot of criticism against Russian foreign policy.

Buzan and Wæver (2006) presented, at the post-Soviet space was centered region (around a great power) and part of a weak super-complex with EU-Europe. Three possible transformations of the regional complex could be identified here:

1. a change in the global position of Russia,
2. internal transformation from centered to balanced,

3. external transformation most likely regarding the border to Europe.

As Buzan and Wæver (2006) presented, at the post-Soviet era brought a great power regional security complex around Russia consisting of two sub-complexes - Caucasus mini complex and Central Asia sub-complex. The Western European great power RSC was included in the weak European super-complex with post-Soviet great power RSC.

Nygren 2010) points out, that Russia and its regional security complex is after more than 20 years after Eastern bloc collapse, influenced by three sub-regions - The European sub-region, the Caucasus regional sub-complex and the Central Asian regional sub-complex.

In literature, there is also declared that in post-Cold War time, "much of what had been referred to as Eastern Europe moved West and became Central and Eastern Europe, and the former Soviet Union became a new international sub-system of states". (Buzan, Hansen, 2009, 180 p.)

Peimani (1998) than states that military factors, especially, affect the degree of dependence of the states in the region on Russia and are the major reason why these states cannot have a life totally independent from Russia, despite their new political independence.

Lake and Morgan then continue that "it is widely assumed that regional conflicts will remain important concerns of policy makers, offering serious threats to peace and to security arrangements while posing awkward and complex problems in security management". (2010, 20 p.)

According to Allison and Johnson, "Russia is today particularly preoccupied with the e.g. of American influence in the region of Central and Eastern Europe." (2004, 17 p.) After period when many states became members of NATO, Russians had to change and develop their security policy in different matter.

According to National security concept of Russian federation from the 2000, main external threats in the international sphere were the strengthening of military-political blocs and alliances, above all NATO's eastward expansion and possible appearance of foreign bases and large contingents in direct proximity to Russia's borders. (National security concept…, 2000)

In this context, the National security strategy of Russian federation presented in 2015 states that the build-up of the military potential of the NATO and the further expansion of the Alliance, and the location of its military infrastructure closer to Russian borders threat her national security. (National security strategy…, 2015) Therefore, the West's stance aimed at countering integration processes and creating seats of tension in the Eurasian region is exerting a negative influence on the realization of Russian national interests.

According to Russians, support of the United States and the European Union for the anti-constitution "coup d'état" in Ukraine led to a deep split in Ukrainian society and the emergence of an armed conflict. Further strengthening of far-right nationalist ideology and deliberate shaping in the Ukrainian population of an image of Russia as an enemy, economic and social crisis were turning Ukraine into a chronic seat of instability in Europe and what is even more important into an instability in the immediate vicinity of Russia's borders. Of course, the events of 2014 and subsequently in February 2022 are a response to the escalation of tensions between the Russian and Ukrainian political leaders and at the same time the culmination of warnings from the Russian side regarding the approach of the "Western security paradigm".

2 METHODOLOGY AND DATA

The methodology used in this paper is presenting results of the detailed research based on the methods of analysis and synthesis, the logical-historical method and the method of

deductive approach. The study in paper is built on a long-time previous researching of documents and academic works focused on RSC around Russia, and consequently on eventual Eastern RSC.

Therefore, the methodology of this paper is predominantly focused on secondary sources, i.e. documents related to the creation, formation and impact of the Complex in the defined territory of Eastern Europe. Logical-historical method allows then studying the pos-Cold War context of Russian federation, using the defined methods.

Analysis of the relevant sources also showed necessity of logical-historical method of research to be implemented in a final research stage in order to correctly synthesize the research outputs.

The underlying hypotheses set out in this research are:

1. The regional security complex around Russia was/has been variable in time and space.
2. Ratio of powers in the RSC around Russia is influenced by the power in its centre (i.e. by the Russia's one covering also the Eastern Europe).
3. The border of the RSC around Russia has shifted simultaneously as the buffer zone of the RSC's central power shifted.

The hypotheses are intended not only to theoretically respond development of the regional security complex around Russia, but reflect eventual security complex in Eastern Europe. The research process showed the need to define new security trends in the development of the regional security complex around Russia, thus, as direct reflection, the research also opened two new dimensions of security theory, i.e. a shift in the theoretical definition of this Complex and shift of the Copenhagen School of Security itself.

As latter suggests, this issue does not require paying attention to all aspects covered by this school. This should be acknowledged despite its interesting attitudes, defining for example the deviation from the traditional understanding of purely military risks and introducing the military security to economic, environmental, social or political security.

3 RESULTS AND DISCUSSION

According to analysis of the relations inside the regional security complex around Russia, it is obvious that the basic structure of this Complex is built on a how the units of the Complex are arranged round Russia and on identifying differences between them. This means, the most significant base lies in distribution of power between these units reflected in friendship or hostility in their mutual security interdependence.

Research focused to verified Hypothesis 1 showed that the critical aspect is the factor of change, i.e. if any of these factors of the Complex change, the whole complex must also be further redefined. Verification of this hypothesis thus proved that the identification, study and analysis of regional security complex around Russia is of practical importance fro assessing and forecasting security developments in this region.

The analyze above made it clear that the analyzed region was historically mainly shaped and influenced by two basic long-lasting developmental stages. The first was the growth and development of the Russian Empire, the second one was the changes in isolation and consequents engagement of Russia with other regions, primarily with Europe. Therefore, following the regional security complex theory, the given region should be perceived as a regional security complex created around the Russian Federation.

Thus, this regional security complex is then undoubtedly formed around the central power, and however today theory does not classify Russia as a global super-power, this country is a constant great power in its surrounding region. The ratio of power in the potential

Eastern RSC is definitely influenced by the power in its centre - Russian Federation. This is confirmed by Trenin (2001), when he presents Russia as a geographical concept, and by Nygren (2010), who states that Russian foreign policy in the CIS region is geopolitical, geo-economic, and geo-cultural. Therefore, Russia's military superiority in the region is also undeniable, confirming thus hypothesis 2.

Regional security complex around Russia concerning the Complex's external borders, is today primarily developed in the context of Russia - EU relations, i.e. in the conditions of the European Union Security Complex. Secondarily, these are Russia's relations with other two above sub-regional complexes, the Caucasus regional sub-complex and the Central Asian regional sub-complex.

Historical analysis of the development of the regional security complex around Russia proved relevance of defining of how this Complex has changed and shaped into the today's security complex recently. As the research made it clear, this RSC around Russia varies in time and geographical space due to varying both internal and external conditions consequently affecting dynamics of the Complex.

Internal causes of the changes in the regional complex could unequivocally be found in the actions of the Complex's central power. This concerns both in proclamation and the subsequent fulfillment of Russia's internal and external security strategy. I believe that regard should be placed on domestic or international conflicts taking place in the area under investigation. However, in this context, it is necessary to examine whether the most important changes in form and dynamics have currently happened within this RSC around Russia or outside the RSC.

As already notices, the research has proved that the further development of the Complex is also related, among other things, to the fact that the European Union and, in particular, the United States of America have become economic or (in some cases) political alternatives for the Eastern & Central European countries. At present, this reality is reflected by the ongoing Ukrainian conflict. This conflict in essence represents the struggle of one past of Ukrainian political spectrum for revival of friendly relations with the Russia and preserving the country under the Russian sphere. On the other hand, this conflict is defined by the other spectrum's attempt to establish pro-European or pro-Atlantic relations with the EU countries and the United States.

The basic security problem within the Complex in this part of the Eastern region lies mainly in the internal instability of Ukraine and, to some extent, in the fact that the Russia refuses to accept the full independence of this state. As an independent state, Ukraine has existed since the Middle Ages and for a short period after the revolution in 1917. The frontiers of the country have also been the result of much of the bizarre clauses, which also correspond to the donation of the Crimea to Ukraine in 1954.

These facts resulted in the fact that in one territory and formation of one state the different territories with different histories and very diverse opinions on how the idea of independence in the country is to be presented.

The current development of relations between the Ukrainians and the Russian Federation, or their relations with the European Union and the United States, have resulted not only in the logical fakt that Ukraine is not a stable country because of the ongoing armed conflict, but what is more important from the security complex theory aspect, the situation has resulted in the movement of the great power's buffer zone. Since it is essential for every super-power to have created a "buffer zone", even in this case, it is clear that the Russia needs to respond to this situation. Russia's perception of own vulnerability has been growing simultaneously with its failure to maintain a forward defense zone bounded by Russian border troops on all the outer CIS states border.

If focusing on the Eastern European region geopolitically, it is worth affirming that

there is a high and logical presumption of the transfer of the Russia's buffer zone from the territory of Ukraine to the border between Ukraine and the Slovak Republic or to the territory of the Slovak Republic. This assumption, however, brings a new situation not only for Slovakia but also for the European Union itself and regional security. The Slovak Republic needs to analyze this situation unambiguously and make it transformed into national foreign policy strategy and into a national security strategy. Meanwhile, the European Union should unequivocally adapt understanding of its security concept to the current developments in Ukraine.

On the theoretical level, this state of affairs points to two main facts. One is that the security complexes formed at the beginning of the new millennium are no longer valid when defining the power of regional complexes and super-complexes. The second fact shows that the security boundaries not only in Eastern Europe, but also in the so-called super complex of Europe (define by Buzan and Wæver in 2003 - 2010) call for their redefinition. Therefore, hypothesis 3 is confirmed because the RSC border around Russia has shifted altogether with the shift of the buffer zone of the Complex central power.

Possibility of forming new Eastern regional security complex opens further academic discussion, though, there is strong believe, that changes in regional security complex around Russia, as defined in literature and analyzed in this paper, also predict strong changes in the field of regional security complex theory in this region.

CONCLUSION

In the post-Cold War era, geographical region around the Russian Federation has gradually changed. This change was evolved by changes inside of Russian Federation, i.e. through changes to individual units as well as through changes to the external borders of the past definition of post-Soviet RSC and European RSC. In this connection, the hypothesis 1 clearly predicting variability of the Eastern European region in the context of changes in regional security complex, was confirmed. There can be clearly stated that the changes in the examined regional security complex that occurred after the end of the Cold War, mainly concerned:

1. Position of the Russian Federation as a super-power in the RSC around Russia.
2. Changes in the sphere of influence in the former Soviet countries.
3. Enlargement of the European Union and North Atlantic Treaty Organization (NATO) up to the borders of the Russian Federation.
4. Sub-regions or countries in conflicts that were part of a previously defined post-Soviet RSC.

Position of the Russian Federation has gradually changed, but despite many internal predominantly economic and societal problems. Nowadays Russia confirmed its super-power position and it is clear now that this power is the driving force behind the transformation of the researched regional security complex.

Collapse of the Soviet Union, imitation of exerting influence on the countries of the former Soviet bloc, EU & NATO enlargement have clearly contributed to a change in the formation of the new RSC around Russia.

As proved above, the post-Soviet regional security complex is changing around the Russian Federation and therefore it can be discussed now whether evolving of a new RSC - Eastern RSC is possible.

Based on the research introduced in this paper, the Eastern RSC could be defined based not on the strict deterrence of all EU Member States, but rather on the concept of a flexible transfer of borders of the security complex formed around the Russian Federation. Therefore, need for academic and scientific discussion about moving buffer zone and about

flexibility of RSC border, is obvious and clear.

BIBLIOGRAPHY

ALLISON, R. - JONSON, L. 2004. *Central Asian Security: The New International Context.* Washington, DC : Brookings Institution Press. 2004, p. 296, ISBN 978-0271-04326-5.

BUZAN, B. - WÆVER, O. 2006. *Regions and Powers. The structure of International Security.* Cambridge: Cambridge University Press. 2006, p. 598, ISBN 978-0511-49125-2.

BUZAN, B. - WÆVER, O. - WILDE, J. d. 2005. *Bezpečnost. Nový rámec pro analýzu.* Brno : Centrum Strategických Studií. 2005, p. 270, ISBN 80-9033-336-2.

BUZAN, B. - HANSEN, L. 2009. *The Evolution of International Security Studies.* Cambridge : University Press. p. 384, ISBN 978-0521-87261-4.

HOFREITER, M. 2016. *Bezpečnostné prostredie súčasného sveta*. *Security environment of current world.* Zlín : Vradim bačuvčík - VerBuM, Retrieved March 15, 2020 from: http://fsi.uniza.sk/kbm/hofreiter/bezpecnostne_prostredie_sucasneho_sveta. pdf.

CHRISTENSEN, T. 2002. *Russian Security Policy According to a Hegelianised Copenhagen School,* Thesis for the M.Sc. in Political Science, Copenhagen : Faculty of Social Sciences, University of Copenhagen. Retrieved March 5, 2020 from: http://www.academia.edu/2918303/Russian_security_policy.

LAKE, D. A. - MORGAN, P. M. 2010. *Regional Orders: Building Security in a New world.* Penn State Press, 2010, p. 406, ISBN 978-0271-04326-5.

NATIONAL SECURITY STRATEGY OF RUSSIAN FEDERATION. 2000. Retrieved August 15 2022 from: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/contentPid/589768.

NATIONAL SECURITY STRATEGY OF RUSSIAN FEDERATION. 2015. Retrieved August 16 2022 from: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.

NYGREN, B. 2010. Russia and the CIS Region: The Russian Regional Security Complex. In *FREIRE, M.R. - KANET, R.E. (eds.) Key Players and Regional Dynamics in Eurasia.* London : Palgrave Macmillan. Retrieved August 10 2022 from: https//doi.org/10.1057/9780230290754_2.

PEIMANI, H. 1998. *Regional Security and the Future of Central Asia: The Competition of Iran, Turkey and Russia.* Boston : Greenwood Publishing Group, 1998, p. 151, ISBN 978-02759-6021-6.

TRENIN, D. I. 2001. *The End of Eurasia.* Moscow : Carnegie Moscow Center Tucker. In *BERNKOPF, N. 1998-9. China-taiwan: US Debates and Policy Choices, Survival 40,* (4): 150-67. Retrieved February 18 2020 from: http://people.duke-edu/~niou/teacheng/Tucker. pdf.

JUDr. Ing. Anna ĎURFINA, PhD. et PhD.
University College Prague - Vysoká škola mezinárodních vztahů a Vysoká škola hotelová a ekonomická s.r.o
Malokrasňanská 2, 831 54, Bratislava
durfina@vsmvv.cz

CONTEMPORARY SECURITY THREATS FOR OUTER SPACE

Marek DVOŘÁČEK

ABSTRACT

The article focuses on the area of space security, specifically on the current changing geopolitical landscape and military anti-satellite capabilities advances in the context of outer space. The first part introduces the rapid development of a once predominantly state-oriented and dominated environment up until the currently diversified multi-stakeholder arena. In the second part, the article focuses on space security and intentional threats to satellite systems, as well as unintentional. The conclusion presents compressed main pillars of the evolution of space security and trends regarding anti-satellite systems.

Keywords: outer space; anti-satellite systems; space security; international security

INTRODUCTION

The importance of the outer space domain, in parallel with cyberspace, is steadily increasing. While in 1966, only a few states were able to produce, launch and manage satellites, half a century later, the situation is diametrically different. Perception of the space domain in not distant past and present has been swiftly changing; its development reflects the importance of stakeholders in the national security paradigm of nuclear confrontation during the Cold War and the modern, increasingly business-oriented, international arena.

Satellite systems have become a pillar of present-day advanced economy and society, and for the military no less — infrastructure serving as "enabler" for complex interconnected systems across various sectors. On the global level, it is, directly and indirectly, influencing billions of people's daily life. Disruption or shutdown of space systems, whether intentional or not, could cause enormously disastrous effects on other key infrastructures and sectors, leading to possible bursts of crises with hardly predictable spill-over effects.

While policymakers and the general population may nowadays come across headlines such as: „China just landed on the far side of the moon: What comes next?" and "US[1] will develop space-based missile defence" merely within the span of two weeks, there are numerous substantial pressing issues to tackle. Therefore, the central aim of this article is to help to orient in the space sector, which has drastically changed over the past decades thanks to new technological progress, business activities and international progress in establishing universal norms.

The analysis serves the purpose of pointing out the evolving space milieu that is often referred to as a new, congested, contested and competitive, vaguely regulated zone with enormous potential.

One of the most dominant variables is the actual number of satellites orbiting planet Earth. While the first one ever to do so was Soviet Sputnik in 1957, currently there are almost

[1] Laid-out new plans are for space-based sensors and other high-tech systems designed to quickly detect and defeat attacks. Outer space has been addressed as "the new warfighting domain", complementary to the prior established United States Space Force, which is the sixth branch of armed forces alongside Army, Marine Corps, Navy, Air Force, and Coast Guard. The proposal of placing missile defence systems in outer space aims to neutralize potential Russian and Chinese hypersonic and cruise missile threats.

5,4 thousand functional active satellites coming from more than 70 countries, according to available data (USC 2022). Due to the shift of the absolute emphasis from traditional military viewing on the space, and the growth of private commercial satellites, the narrative is now multidimensional. Nevertheless, Earth's orbit is on the brink of massive change. According to estimates of The World Economic Forum, it is expected increase is almost tenfold over the next decades, up to $1 trillion in the next two decades (WEF 2022).

The potential of growth for the industry and subsequent application of services, is on one hand an opportunity, on the other hand a risk associated with pollution and threat of collision. Such fundamental change is attracting various actors, some of which may posse unwelcome risks, incidents and examples are occurring even today.

1 EVOLUTION OF THE DOMAIN

Undoubtedly one of the most prominent incidents in 2018 was Swarm Technologies, a fairly new actor in the field hoping to eventually send up to 100 satellites into orbit, with the vision of beaming global internet coverage to Earth for connected devices. At the beginning of 2018 Indian PSLV rocket launched a payload consisting of four small testing satellites. The catch is hidden in a lie. Swarm Technologies could not get a license from US Federal Communication Commission (FCC) to send such technology into space. The American authority was worried that SpaceBEEs were too small to track and thus dangerously inclining to a possible collision with other satellites. The US authority is not only responsible for designating radio frequencies for domestic companies but for authorization to any domestic payload into orbit. This is even more important due to state responsibility for the actions of its domestic actors in outer space according to international law (Koren 2018).

Space start-up Swarm Technologies thus launched satellites without governmental approval while lying to the Indian rocket launcher provider that they were awarded a certificate. The such incident happened for the first time in "space age", very likely not for the last time. US Treasury later charged Swarm Technologies for $900 000 because of the unauthorized launch. Chief of Enforcement Bureau of FCC claims they "will aggressively enforce FCC's authorization requirements companies seek to get" and that "these important obligations protect other operators against radio interference and collisions, making space a safer place to operate (ibidem).

In any case, this is just a fragment of current affairs. However, what are the overarching trends transcending since the beginning of the space age? How did humankind come to this stage?

While terms such as defence, nuclear deterrent, and strategic parity were the core for utilizing outer space since the first ballistic missile experiment, whereas current "NewSpace" era (or "Space 4.0") is focusing on commercialization. National state, as a dominant player, has lost its previous monopoly on technology; on the contrary, commercial entities, non-profit organizations, and the scientific and academic sphere are continuing their rapid growth in the use of space. The private sector is now a central player in progress in space, with the value of the entire industry amounting to $424 billion as of 2020 according to the World Economic Forum (WEF 2022). In the next three decades, an increase of nine times the current amount should occur.

Cloud services, cheaper process performance, and component miniaturisation allow more and more actors to use data previously generated by governments or large telecommunication companies. Thanks to that, we are now at the beginning of a large renaissance start-up with the application of space services with commercial and social coverage. In the debate on the existing space policy and space-based business, it is said that space has become privatised, democratic, and proliferated by actors.

Earth-based systems became so interdependent and reliant on their spaced-based counterparts that the socio-economic consequences of any partial disruption of availability or integrity could be dramatic. Just navigational space data and signals are responsible for an estimated 10% of the European Union's GDP, roughly $2 trillion (ESPI 2018). Any potential, even brief, disruption would be as destructive as a blackout of power grid, mainly due to the proper functioning of a large number of associated economic and civil services. From the point of near future and exponential spreading of autonomous systems, satellite navigation is crucial to support such a ground-based application. Moreover, large scale weather and meteorological phenomena monitoring in the atmosphere has a significant impact on economic growth. 25-30% of the gross domestic product in developed countries is sensitive to weather changes, not to mention other unmet social benefits. EUMETSAT is a European intergovernmental organisation with purpose of supplying weather and climate satellite data, images and products for national meteorological services of European member states. Weather forecasts in the EU substantially support €43 billion in value-generating sectors a year, such as transport, energy, agriculture, tourism, food and construction (EUMETSAT 2021).

From these examples, it is quite clear the significance of satellite systems for socio-economic purposes. In addition, as stated above, the first decades of the space age were driven particularly by Soviet and American military endeavours that are highly connected to ballistic missile technology progress. Intelligence, reconnaissance, surveillance (ISR) and nuclear detection satellites established the backbone of national defence, which is overall deepened interdependency through modernisation and revolution in military affairs. Since 2019 outer space as such has become one of the theatres of warfare covering each aspect of military operation from planning and preparations to final assessment[2]. Modern warfare would be mainly sent back to the analogue first part of the 20th century without such operational capabilities (Ayan and Ladd 2022).

2 SPACE SECURITY

The previous chapter ended with an invitation to further explain the concept of space security. Although this concept does not have a universally accepted definition, there has been substantial a reassessment of the terminology and perception throughout the years. For the prestigious Space Security Index, space security is simply reflected as "safe and sustainable access to space and its use, as well as freedom from space-based threats." This definition is based on the principles of space security laid down in the 1967 Outer Space Treaty[3], according to which outer space should remain freely available to all for peaceful use now and in the future. The authors themselves argue that the definition should not defend a particular state actor or private entity but underline the importance of responsible use of space by all parties. Such a broad definition includes the sustainability of the cosmic environment, the physical and operational integrity of artificial objects in the domain and their terrestrial segment. Last but not least, it includes the security on Earth from the threats and natural hazards of the cosmic environment.

[2] North Atlantic Treaty Organization uses space services for a position, navigation and timing (precision strike, network timing, force navigation), integrated tactical warning and threat assessment (force protection, attribution, missile defence), environmental monitoring (mission planning, munition selection, weather forecast), communication (command and control, autonomous vehicles), ISR (targeting, battle damage assessment) and identification. An attack to member state's satellite would trigger Article 5 of the North Atlantic Treaty (NATO 2022).

[3] Formally, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

In the introduction to the Handbook of Space Security Policies, Schrogl (et al. 2015) defines space security as a two-dimensional issue, in other words, security in space and security on Earth from space. This two-dimensional conception encompasses all aspects related to the ensuring space operations are as safe as possible, and the use of the environment is protected, achieving the goal of benefiting and strengthening people on Earth.

Although the definition is still the subject of discussion and some variations have developed, its substance is constantly changing. Traditionally, during the Cold War, space security has been perceived by military terms as a strategic balance. However, the fundamental aspect, which has remained so far, is ensuring the contribution and continuity of satellite operation into the broader defence and security systems at the national level, and thus maintaining international stability and balance of power.

According to Moltz (2011), the definition of space security is the ability to launch and operate satellites outside the Earth's atmosphere without external interference, damage or destruction.

Such a narrow targeted and traditionally oriented definition of security, implies referring to threats against the state, in particular the military threat by the armed forces of another state. However, according to Sheehan (2015, p. 7), it does not reflect the "everyday reality of the people on Earth". That has led to the gradual evolution of the understanding of the space security concept (as well as the general term security itself).

The current two-dimensional understanding of space security (as safe and sustainable access to space and its use, as well as freedom from space-based threats) was enriched by another (third) dimension - the use of outer space to support the general security of people on Earth through, for example, communications for rescue and crisis management in the event of natural disasters, monitoring extreme weather conditions and improving effective agricultural production.

Another practical three dimensions of space security are summarized by Mayence (2010, p. 35). Space security means at the same time:

- Outer space for security: the use of space systems for security and defence purposes;
- Security in outer space: how to protect space assets and systems against natural and/or human threats or risks and to ensure sustainable development of space activities;
- Security from outer space: how to protect human life and Earth’s environment against natural threats and risks from outer space.

3 THREATS AND RISKS

Both definition of the Space Security Index and Mayence indicates that a variety of trends from inside and outside the space sector are challenging the status quo, recognizing the one-of-a-kind fragile status of outer space, implying a collective strive to secure essential principles. The ecosystem shifted over the past decades with new technical concepts, innovations, and a wave of competition. Weeden and Samson (2018) note that growing reliance on outer space for national security creates an incentive for some states to develop counterspace capabilities that can be used to disrupt, deny, degrade, or destroy space systems, thus partially overcoming the asymmetrical position of a more advanced or powerful adversary - alternatively using the technology as a potential deterrent.

Challenges to space security and space infrastructure include an ever-growing number of debris fragments, radio interferences, space weather hazards and anti-satellite technologies (ASAT). While solar radiation and geomagnetic storms unintentionally negatively affect human activities, kinetic (direct ascent) counterspace military capability is an entirely different case, a demonstration of force.

As mentioned before, states and their militaries have been testing anti-satellite means; during the first half of the 1960s, the United States undertook several tests of nuclear explosions in the upper parts of atmospheric levels, where the effects and impacts were substantially different from a ground explosion. The STARFISH is a series of tests, one of the most well-known nuclear explosion experiments in the fringe of outer space, before banning them effectively. Surprisingly, the primary mechanism of satellite destruction was not an explosion or pressure wave but consequently increased radiation in the given area. The explosion created artificial radiation strips damaging passing satellites and their electronics (Hostbeck 2015).

As the most critical security element in outer space and its application to Earth-based systems, satellites are threatened by three major factors – anti-satellite technologies, cyber threats, and last but least, space debris. The author chose this particular framework, which is going to be explained further on.

3.1 ANTI-SATELLITE SYSTEMS

Hostbeck (2015) argues that the path leading to conflict in space and through space begins on Earth, and since military strength capability is closely related to technology and systems in space, the conflict can spread into the domain. According to him, anti-satellite missiles are designed only for one purpose, to eliminate an enemy object. Nevertheless, the renowned Space Security Index divides anti-satellite weapons into several categories, some of which are not aiming to destroy but rather disrupt, deny, or degrade without being genuinely noticeable and easily attributed.

In addition to the non-existent weapon systems on orbit, those categories incorporate Earth-based conventional direct-ascent, nuclear, and directed energy technologies (laser or microwave systems). Mentioned conventional rocket is then divided into the kinetic energy "hit-to-kill" (which requires extreme precision guidance), with an explosive head or with material that dissipates on the orbit and collides with the satellite. The result of these technologies is not just a danger to the sustainability of the environment due to the accumulation of space debris, but rather mutual distrust. According to the index, in 2017 and 2018, the development of exoatmospheric[4] anti-satellite weapons continued to move forward for advanced actors, especially in the area of directed energy technologies.

Although there has not been registered an intentional, impactful hostile incident using anti-satellite systems yet, teasing, testing and experimenting mainly with non-kinetic capabilities are being actively used often in current military operations.

The development of anti-satellite systems is particularly evident as a way of balancing asymmetrically spread powers, according to for example Kleinberg (2007), the physical vulnerability of satellite systems means to the United States and their strategic advantage that any attack on these systems would paralyze the economic and military spheres, and thus meant a declaration of war. Dolman and Cooper (2011) demonstrate this strategic advantage (and dependence) of the US in the comparison of the use of guided ammunition. During the Vietnam War, the United States used devastating but inaccurate B-52 bombers with large-scale collateral damage. During Operation Desert Storm, 8% of the ammunition was

[4] While there are no advanced weapon stations confirmed, micro and nanosatellites with manoeuvrability could be potentially used as “mines” or kamikazes. As demonstrated, for example, by the Chinese nanosatellite BX-1 test and Russian Luch/Olymp-K activities in the geostationary orbit. The latter example indicates an intention to approach both military (in the case of the French-Italian military communication satellite) and commercial communication satellites (Weeden and Samson 2022), which is a hazardous and uncommon move given the modus operandi of the geostationary orbit regime. The highly likely intention was to move the satellite close enough to the foreign satellite and get into the ground terminal uplink window.

precision-guided, however, without the use of GPS[5]. About 70% of used munition in Operation Iraqi Freedom was precision-guided, with half of the weapon systems using GPS. In Desert Storm, GPS was used by 5% of aircraft, yet during Operation Iraqi Freedom, it was all of them. According to the authors, the first mentioned operation showed how beneficial this technology is to the army, so GPS-enabled electronics were quickly purchased and installed. Last but not least, in Operation Iraqi Freedom, each team had at least one GPS receiver to determine the exact location.

This was a significant Chinese successful breakthrough after the Cold War. In 2007, the Chinese People's Liberation Army demonstrated its anti-satellite technology at its full potential. They began developing systems in the 1990s, and after several failed tests since 2004, they were able to shoot down their own inoperative meteorological satellite, Fengyun-1C. At an altitude of 864 kilometres above sea level, the SC-19 rocket, which according to available information, should be modified by the ballistic missile DF-21, hit the mark. The shooting, or rather the shattering, has caused a considerable upsurge in the international arena. Mainly because Chinese created 27 000 pieces of space debris, threatening the entire ecosystem, and a substantial portion of it will remain there for the next 35 years. The United States also downed its satellite a year later; pollution was, fortunately, multiply minor (Wong and Fergusson 2010). The SM-3 missile shot down a reconnaissance satellite at the height of about 240 kilometres and created 174 traceable pieces of space debris. However, by the end of 2009, they had descended into the atmosphere. The missile is also part of the Aegis Integrated Air Defense System. Last but not least, Russia has undergone at least five successful PL-19 / Nudol system tests since 2015. Although rockets should be officially part of missile defence, the US intelligence community suspects it is primarily the anti-satellite system (Young 2022).

The latest intercept test of the Nudol occurred on November 15, 2021. Nudol intercepted and destroyed Cosmos 1408, a defunct Russian military satellite known as the Soviet Tselina-D signals intelligence satellite. Destruction subsequently generated approximately 1 500 pieces larger than 10 cm that have been catalogued and are expected to stay in orbit for years (Weeden and Samson 2022).

3.2 CYBERSECURITY THREATS

Text Increasing traffic in the orbit also brings forward safety issues associated with manoeuvrability and control of satellites, notably due to possible collision hazards with other objects. Although cybersecurity is indirectly linked to space, this technical issue is increasingly accentuated in the context of space systems. Harmful interference may not destroy the satellite (temporary or permanent damage may occur) but limit or disable its functionality, effectively alternating its intended purpose. Compared with ASAT, exploiting cyber vulnerabilities within a space system is a more refined form of combat. Due to the widespread use of computing technologies and automatization in the space sector, it doubles down on cybersecurity threats. They take two forms; the first one is aiming satellites in orbit, and the second one terrestrial devices (control centres and parabolic antennas designed to receive and transmit signals between centre and satellite) (Livingstone and Lewis 2016).

Interfering the signal is meant an attempt to degrade or disrupt the connection between the satellite and the user. It is a rather primitive but effective cybernetic attack on satellite functionality, which has been exploited for decades. It is deliberate interference of the transmission and reception of a signal using radio-frequency noise and electromagnetic signals. Simple jammers transmit a signal that ignores the satellite's specificity but only

[5] The Global Positioning System, which was created for military purposes, but its civilian use has been met by almost everybody in modern society - whether using mobile or vehicle navigation or purchasing goods that have arrived at the destination via maritime transport.

attempts to overwhelm it; more complicated jammers then use techniques that use signal or satellite receiver properties to block specific functionality on multiple frequencies at the same time (Shackelford and Russell 2015). In this case, the interference device transmits electromagnetic energy at the same radio frequency as an authorised satellite-operated device, so the satellite is consequently unable to capture and operate the correct authorised signal because it is overwhelmed by the false.

Whether threatening to steal, compromise data, or "disable", satellite systems are prone to a wide range of cyber-attacks. According to some experts, this is the biggest weakness of whole system in general. In particular, cyber-jamming is a growing problem for both commercial actors and governmental agencies alike. Important to note here is that it is deliberate, intentional, state-sponsored signal interference aimed at fulfilling military, political or social goals (Robinson 2016). Other forms include cyber-spoofing (sending false data to the system) or rare and complex advanced persistent threat techniques - cyber-hijacking (Dobryakova, Lemieszewski and Ochin 2016). However, the remaining fact is that according to the International Telecommunication Union (ITU) growing number of actors and satellites responsible for incidents create a pressure on a limited number of wave frequencies. The unintentional overlay of the signal causes up to 85% of satellite signal failures.

Moreover, it has become an increasingly thorny genuine problem for satellite operators, although not epidemic. A signal overlay occurs at a time when devices on different satellites use the same radio frequency and their position is relatively close to each other. This is particularly true in the most commonly used levels of the orbit where there is a high presence of satellites. Specifically, the lucrative geostationary orbit is mentioned in this issue. In addition to its agenda and regulations at the World Radiocommunication Conference in 2015, the ITU has prepared an update of the rules for creating conditions for the application of new and existing technologies in the use of the radio spectrum. All this is in the context of improving the situation (Marentes 2016).

The ground segment of the space systems that the satellites operate, monitor, and communicate with through parabolic antennas is entirely dependent on the cyber domain. Telemetry, monitoring and management of satellites are managed by operators, servers, desktops and specialised software systems. These information systems then process and transmit information to the satellite within the complex. Moreover, as the human factor is part of this vast system, infection and gradual spread in the system can quickly occur (Housen-Couriel 2016). Against this, Slann (2016) proposes prevention by investing in infrastructure security, data and systems controls, and cybersecurity training for staff.

Although this chapter might seem rather theoretical, there is an example of a successful cyber-attack. While a majority of commercial subjects withhold information regarding successful cyber-attack, nota bene military or civil institutions, to protect their customers and financial interests. Nevertheless, there is documented incident from 24 February 2022, approximately an hour before Russia launched its military campaign to occupy Ukraine. Commercial communications company Viasat was hit by a malware attack dubbed “AcidRain” that effectively preventing thousands of Viasat ground terminals, modems, from accessing the company’s European KA-SAT network (UK GOV 2022). This loss of the network of geostationary communications satellites had a widespread impact on Central Europe, be it personal and commercial internet users (e.g., wind farms), as well as the Ukrainian army that used Viasat’s services for its strategic communication. Ukrainian Deputy Chairman of the State Service of Special Communications and Information Protection, Victor Zhora, noted that the cyber-attack resulted in a significant loss in communications at the beginning of the war. Viasat’s ground terminals were taken offline by an apparent software supply chain attack delivering the wiper malware (Cohen 2022).

4 SPACE DEBRIS

Both anti-satellite weapons and cyber-attacks (targeting the terrestrial segment of the space infrastructure in particular) threaten the infrastructure functionality directly, yet at the same time for the consequences. Regarding the sustainability of space use, we find ourselves at a critical time that is threatened by space debris. The debris consists of remnants of past missions, parts of launchers and wreckages of broken satellites. The major problem is also the potential for the massive proliferation of debris caused by cascade chaining of the debris (Harrison, Johnson and Roberts 2018).

The so-called Kessler cascade Syndrome is a condition of a rapid reduction in the usability of the orbit due to an exponential growth of objects in the domain. Debris or any small fragments threaten active satellites before breaking and generating more debris, which may subsequently accumulate (Drmola and Hubik 2018) more debris. Since such fragments, due to laws of physics, could remain in orbit for many years (on geostationary orbit indefinitely), hypothetically speaking, there is a potential to weaponise this effect in the conflict. Not only would that mean limiting or devastating the functionality of any satellite systems, but it would also mean outraging the international scene and possible spill-over conflict.

Each and every space mission creates, in fact, some amount of debris, uncontrollable small objects as a result of an accident or as a residual and unwanted consequence of loading the cargo into orbit[6]. The previously introduced Chinese anti-satellite weapon test in 2007 rapidly increased the amount of debris; overall, the number of objects in orbit has increased since the beginning of the cosmic age without any meaningful instrument for cleaning the domain. The whole ecosystem is affected, regardless of the origin of the actor or his interests and assets in outer space. The US Department of Defense, through its Space Surveillance Network (SSN), records in the catalogue 15 000 objects larger than 10 centimetres. They are moving through space at about 7.8 kilometres per second and can cause considerable damage to the orbit. According to mathematical models, however, garbage is far more than 300 000 pieces with a diameter of more than one centimetre[7] and several million even smaller. However, it is impossible to track and catalogue it with the existing technique (Czysz, Bruno and Chudoba 2018).

There has been a noticeable reduction in the annual increase in space trash in the last decade of the last century due to national mitigation efforts. On the other hand, even a one-off event, like the Chinese 2007 test destroying a non-functional meteorological satellite, is enough to prevent structural changes from reversing the acceleration of orbital pollution. Although there are concepts of programs for active orbital cleaning, it is because of the sensitivity of the technology to the state that has not yet been explored. For the time being, the United Nations Committee on Peaceful Use of Outer Space (COPUOS) has prepared universal guidelines for mitigating the impact of space debris (UNOOSA 2017). The main impetus here is the effort to limit unwanted litter at the start of the mission, leaving sufficient fuel to expel the atmosphere before the end of life, thus limiting the long-term presence of carrier parts and satellites if their role is already fulfilled.

---

[6] The fragments originate in particular from the central part of the carrier rocket, which is detached from the cargo and, together with other released hardware particles, is allowed to be drifting in space. From the point of view of the satellites themselves, about 45% of all disruptions of active satellites are based on problems with propulsion systems, 29% are consciously led to the atmosphere where they are burned due to obsolescence, endlessness or end of life, 20% are unknown causes of technical nature, 4% batteries and 2% is a random collision (SSI 2019).

[7] According to the European Space Agency, it should be more than 700,000 pieces of debris larger than 1 centimetre in orbit that can damage any functional, active satellite.

CONCLUSION

The context of Space Security has been developing ever since the Soviets launched artificial object for the first time outside Earth's atmosphere in 1957. While there has not been a general agreement on the definition, the United Nations through Outer Space Treaty recognised two main goals: sustainable and safe access to space and its use as freedom from space-based threats. Although the UN appeal for peaceful use of outer space, there has not been a formal policy declaration regulating kinetic or directed energy weapon technologies yet; there is just regulation of nuclear explosions and placement of nuclear weapons in the upper atmosphere. Given this, some argue that the sense of urgency is less than typical in arms discussions and, therefore, the focus should be on prevention rather than control.

Direct-ascent kinetic weapon systems may seem brute force compared with cyber threats, particularly jamming satellites' signals that occur regularly. Nevertheless, there is no recorded intentional use of anti-satellite technology during conflict aiming to destroy an enemy satellite, only to deny its military application to the ground. Other than intentional threats toward satellite systems in orbit, there are two other major problems. The first one is a growing amount of debris threatening the middle and long-term sustainability of the domain; the second one is the contemporary issue of radio frequency disturbance. That is caused by both a growing number of actors and satellites in orbit, which might be problematic when in close proximity.

Sustainability is a focal point for many on the highest level of importance due to commercialisation, privatisation and growing satellite population, which is projected to grow ten times in the upcoming decade – from current almost 1 900 to 19 000. With the entry of 5G and autonomous vehicles in a more prominent role, precise undisturbed navigation and other satellite applications are going to be indispensable. It puts pressure on states on the global scale to collectively decide how to solve space debris and frequency disturbance problems.

Another problematic issue is the connection with significant research and development of a broad range of counterspace capabilities in multiple countries. There is no agreement or "manual" addressing the issue of belligerent behaviour during hostilities regulating when and under what circumstances it is lawful for nations to resort to hostilities in or through space.

Outer space is vital to various sectors of human activities on Earth, for which transparency and confidence among states with anti-satellite technologies, in particular, play an essential part. Any potential use of force would have unforeseen consequences and repercussions for everybody down on Earth for generations to come. Clarifying existing international law applicable to military uses of outer space and generating a new norm is an essential imperative to establish proper long-term widely accepted norms in the light of contemporary security threats - especially given the fragile nature of the current status quo facing anti-satellite technologies, cyber threats and space debris.

LIST OF BIBLIOGRAPHICAL REFERENCES

COHEN, Sam, 2022. AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat. New York University School of Law [online]. [cit. 2022-09-15]. Available: https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat/

CZYSZ, Paul A, Claudio BRUNO and Bernd CHUDOBA, 2018. Future Spacecraft Propulsion Systems and Integration: Enabling Technologies for Space Exploration. Third edition. Springer. ISBN 978-3-662-54742-7.

DOBRYAKOVA, Larisa, Łukasz LEMIESZEWSKI and Evgeny OCHIN, 2016. The vulnerability of unmanned vehicles to terrorist attacks such as Global Navigation Satellite System spoofing: Scientific Journals of the Maritime University of Szczecin. Scientific Journals of the Maritime University of Szczecin [online]. [cit. 2022-09-02]. DOI: 10.17402/135. ISSN 2392-0378.

DOLMAN, Everett C and Henry F COOPER, 2011. Old Thoughts, Increasing the Military Uses of Spacer. Toward Theory of Spacepower [online]. [cit. 2022-08-21]. Available: http://ndupress.ndu.edu/Portals/68/Documents/Books/spacepower.pdf

DRMOLA, Jakub a Tomas HUBIK. 2018. Kessler syndrome: System dynamics model. Space Policy. DOI: 10.1016/j.spacepol.2018.03.003. ISBN 10.1016/j.spacepol. Available: http://linkinghub.elsevier.com/retrieve/pii/S0265964617300966

ESPI, 2018. Cyber Security: High Stakes for the Space Sector. European Space Policy Institute [online]. Available: https://www.espi.or.at/briefs/cyber-security-high-stakes-for-the-space-sector/

EUMETSAT, 2021. EUMETSAT Destination 2030. European Organisation for the Exploitation of Meteorological Satellites [online]. Available: https://www.eumetsat.int/media/48513

HARRISON, Todd, Kaitlyn JOHNSON and Thomas G. ROBERTS, 2018. Space Threat Assessment: 2018. Center for Strategic and International Studies. Available from: https://www.csis.org/analysis/space-threat-assessment-2018

HOSTBECK, Lars, 2015. Space Weapons: Concepts and their International Security Implications In: SCHROGL, Kai-Uwe, Peter L. HAYS, Jana ROBINSON, Denis MOURA a Christina GIANNOPAPA. Handbook of Space Security: Policies, Applications and Programs. New York: Springer. ISBN ISBN 978-1-4614-2028-6.

HOUSEN-COURIEL, Deborah, 2016. Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica. DOI: 10.1016/j.actaastro.2016.07.041. ISBN 10.1016/j.actaastro.2016.07.041. Available: http://linkinghub.elsevier.com/retrieve/pii/S0094576516301552

JAPPC 2022. Collective Defence in the Space Domain. Joint Air Power Competence Centre. [online]. Available: https://www.japcc.org/articles/collective-defence-in-the-space-domain/

KLEINBERG, Howard, 2007. On War in Space. Astropolitics. DOI: 10.1080/14777620701544600. ISBN 10.1080/14777620701544600. Available: https://www.tandfonline.com/doi/full/10.1080/14777620701544600

Koren, Marina. 2018. Launching Rogue Satellites Into Space Was A ‘Mistake’. The Atlantic [online]. https://www.theatlantic.com/technology/archive/2018/09/spacebees-swarm-unauthorized-satellite-launch/569395/.

LIVINGSTONE, David and Patricia LEWIS, 2016. Space, the Final Frontier for Cybersecurity?. Chatham House - the Royal Institute of International Affairs. Available: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity

MARENTES, Ruben, 2022. Satellite Services and Interference: ITU International Satellite Communication Symposium. In: International Telecommunication Union ITU [online]. [cit. 2022-09-04]. Available: https://www.itu.int/en/ITUR/space/workshops/SISS-2016/Documents/Intelsat.pdf

MAYENCE, Jean-Francois. 2010. Space Security: Transatlantic Approach to Space Governance. In: ROBINSON, Jana, Matthew Paul SCHAEFER, Kai-Uwe SCHROGL a

Frans VON DER DUNK (eds.). Prospects for Transparency and Confidence-Building Measures in Space. European Space Policy Institute. [online]. Available: https://www.files.ethz.ch/isn/124817/ESPI_Report_27_online.pdf

MOLTZ, James Clay. 2011. The politics of space security: strategic restraint and the pursuit of national interests. 2nd ed. Stanford: Stanford University Press. ISBN 978-0-8047- 7858-9

NATO, 2022. NATO's approach to space. North Atlantic Treaty Organization [online]. Available: https://www.nato.int/cps/en/natohq/topics_175419.htm

ROBINSON, Jana. 2016. Governance challenges at the intersection of space and cyber security. The Space Review [online]. [cit. 2022-08-28]. Available: http://www.thespacereview.com/article/2923/1

SHACKELFORD, Scott J. and Scott J.D RUSSELL, 2015. Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector. In: Florida International University College of Law Review [online]. Florida: Florida International University College of Law, s. 365-398 [cit.2022-08-28]. Available: http://ecollections.law.fiu.edu/lawreview/vol10/iss2/16

SHEEHAN, Michael, 2015. Defining Space Security. In: SCHROGL, Kai-Uwe, Peter L. HAYS, Jana ROBINSON, Denis MOURA a Christina GIANNOPAPA. Handbook of Space Security: Policies, Applications and Programs. New York: Springer, s. 7-22. ISBN ISBN 978- 1-4614-2028-6.

SCHROGL, Kai-Uwe, Peter L. HAYS, Jana ROBINSON, Denis MOURA and Christina GIANNOPAPA. 2015. Handbook of Space Security: Policies, Applications and Programs 1. New York: Springer. ISBN 978-1-4614-2028-6

SLANN, Phillip A, 2016. Anticipating uncertainty: The security of European critical outer space infrastructures. DOI: 10.1016/j.spacepol.2015.12.001. ISBN 10.1016/j.spacepol.2015.12.001. Available: http://linkinghub.elsevier.com/retrieve/pii/S0265964615300163

SSI, 2019. Space Security Index 2019 [online]. [cit. 2022-05-14]. 978-1-927802-26- 7. Available: https://secureservercdn.net/50.62.89.104/9ac.6b8.myftpupload.com/wp-content/uploads/2019/10/SSI2019ExecutiveSummaryCompressed.pdf

UK GOV, 2022. Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion. National Cyber Security Centre, Government of the United Kingdom [online]. [cit. 2022-05-14]. Available: https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion

UNOOSA. 2017. Guidelines for the long-term sustainability of outer space activities: Working paper by the Chair of the Working Group on the Long- term Sustainability of Outer Space Activities. United Nations Office for Outer Space Affairs [online]. Available: http://www.unoosa.org/res/oosadoc/data/documents/2017/aac_1052017crp/aac_1052017crp_26_0_html/AC105_2017CRP26E.pdf

USC, 2022. UCS Satellite Database. Union of Concerned Scientists. National Cyber Security Centre, [online]. [cit. 2022-09-15]. Available: https://www.ucsusa.org/resources/satellite-database

WEEDEN, Brian and Victoria SAMSON, 2018. Global Counterspace Capabilities: An Open Source Assessment [online]. [cit. 2022-05-14] Available: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf

WEEDEN, Brian and Victoria SAMSON, 2022. Global Counterspace Capabilities: An Open Source Assessment [online]. [cit. 2022-05-14] Available: https://swfound.org/media/207350/swf_global_counterspace_capabilities_2022_rev2.pdf

WEF, 2022. Space: Space Commercialization. World Economic Forum [online]. [cit. 2022-09-15]. Available: https://intelligence.weforum.org/topics/a1Gb0000000pTDUEA2/key-issues/a1Gb0000002KWrHEAW

WONG, Wilson and James G FERGUSSON, 2010. Military space power: a guide to the issues. Santa Barbara, Calif.: Praeger, 158 p. Contemporary military, strategic, and security issues. ISBN 03-133-5680-7.

YOUNG, Makena, 2022. Russia Tests Nudol Anti-Satellite System. Missile Threat [online]. Available: https://www.csis.org/analysis/tracking-developments-counterspace-weapons

Mgr. Marek DVOŘÁČEK
Lidická 899, Lanškroun, 56301, Česká republika
415023@mail.muni.cz

UPLATŇOVANIE PRINCÍPU EKONOMICKEJ EFEKTÍVNOSTI VO VEREJNOM SEKTORE A OSOBITNE V OBRANE

APPLICATION OF THE PRINCIPLE OF ECONOMIC EFFICIENCY IN THE PUBLIC SECTOR AND ESPECIALLY IN DEFENCE

Viera FRIANOVÁ

ABSTRACT

This paper deals with the issue of applying the principle of economic efficiency in the public sector and especially in defence as one of its part. The author presents theoretical and empirical findings from the researched issue. The first chapter of the paper contains theoretical starting points of the researched issue. The author presents the current approaches of different authors to defining the problem of efficiency, resp. inefficiency in the public sector. The content of the second chapter of the paper is to clarify the problem of efficiency in the defence sector. The final part of the contribution contains conclusions that could contribute mainly to the further development of the theory, but also recommendations and suggestions that could find their further practical use.

Keywords: efficiency, public sector, defence, inefficiency, effectiveness of defence spending

ÚVOD

Problém efektívnosti, resp. neefektívnosti patrí k vysoko aktuálnym problémom nielen súkromného ale aj verejného sektora. Keďže zdroje sú vzácne, aj rozhodovanie manažérov verejného sektora je často výberom z alternatív a hľadaním odpovede na otázku, ako disponibilné zdroje ekonomicky racionálne použiť. Otázkami ekonomickej efektívnosti sa zaoberajú nielen ekonómovia, ale aj vládni predstavitelia, ktorí pri svojom rozhodovaní hľadajú odpoveď na otázku, či prostriedky vynaložené v rámci verejného sektora prinesú očakávaný efekt.

Skúsenosti z praxe potvrdzujú, že medzi aktuálne výzvy vo verejnom sektore patria i meniace sa očakávania verejnosti po službách štátu (vrátane zaistenia obrany a bezpečnosti) a spôsoboch ich poskytovania v prostredí s obmedzenými, a teda vzácnymi zdrojmi. V ostatnom období sa tak stále výraznejšie poukazuje najmä na požiadavku ekonomickej efektívnosti, a s ňou súvisiacej účelnosti, hospodárnosti, transparentnosti, a v neposlednom rade i znižovania korupcie.

Hlavným cieľom predloženého príspevku je prezentovať výsledky uskutočneného teoretického a empirického skúmania predmetnej problematiky, pričom pozornosť autorky je sústredená najmä na problém uplatňovania princípu ekonomickej efektívnosti vo verejnom sektore na Slovensku a osobitne v obrane ako jednej z jeho neoddeliteľných súčastí. Parciálnymi cieľmi príspevku je vymedziť kľúčové pojmy, objasniť ich vzájomné súvislosti, priblížiť problém neefektívnosti, uviesť jeho príčiny a možné riešenia, vysloviť závery a formulovať odporúčania pre rozvoj teórie a pre prax.

Príspevok je rozdelený do dvoch kapitol, obsahom prvej kapitoly je prezentovanie aktuálnych prístupov k objasňovaniu problematiky efektívnosti verejného sektora, vrátene podstaty a príčin neefektívnosti. Obsahom druhej kapitoly príspevku je objasnenie problému

efektívnosti v odvetví obrany. Autorka sústreďuje pozornosť najmä na efektívnosť inštitucionálneho charakteru, prezentuje tak najmä mikroekonomický pohľad na verejný sektor.

1 VÝCHODISKÁ SKÚMANEJ PROBLEMATIKY

Predpokladom skúmania danej problematiky je vymedzenie kľúčových pojmov, ako sú: efektívnosť, efektivita, racionálne správanie (konanie), hodnota (úžitok), ako aj objasnenie ich vzájomných súvislostí.

Efektívnosť považujeme za kľúčový princíp racionálneho hospodárenia so zdrojmi, ako v súkromnom, tak i vo verejnom sektore. Samotný pojem efektívnosť (rovnako ako pojmy efektivita, účinnosť, úžitok, prínos, či produktivita) sa vo všeobecnosti spája s ekonomickou efektívnosťou, ktorá nadobúda z hľadiska cieľa rôzne podoby. V literatúre sa preto pri snahe vymedziť daný pojem môžeme stretnúť s rôznymi pohľadmi autorov.

Napríklad Nemec a kol. (2011) definujú efektívnosť/produktivitu ako „pomer medzi očakávanými výsledkami a nákladmi potrebnými na ich dosiahnutie – dosahovanie maximálneho výstupu z daných vstupov alebo minimálnych nákladov na dosiahnutie požadovaného výstupu. Na jej meranie sa najčastejšie používajú hraničné ukazovatele pomeru vstupov a výstupov, príp. ich hraničná podoba zmeny výstupu pri malých nárastoch vstupov“.

K uvedenej spojitosti efektívnosti a produktivity vyjadruje svoj názor aj Vorlíček, (2008), ktorý však namiesto pojmu efektívnosť používa pojem efektivita. Podľa neho efektivita vyjadruje mieru plnenia sledovaných cieľov. „Z ekonomického hľadiska ide o vzťah medzi výnosmi a nákladmi... tzn. efektívna je taká činnosť... kde je čistý úžitok (t. j. rozdiel medzi výnosmi a nákladmi) najvyšší, teda kde výnosy čo najviac prevyšujú náklady“. Zároveň zdôrazňuje, že je potrebné odlišovať efektivitu od produktivity, lebo je medzi nimi len jednosmerný vzťah (teda ak sa zvyšuje, či naopak znižuje efektivita, zvyšuje sa, či naopak znižuje vždy i produktivita), ale nie ekvivalencia (teda ak sa zvyšuje, či naopak znižuje produktivita, nemusí sa nutne zvyšovať či znižovať i efektivita – zvýšenie, či zníženie produkcie môže mať i iné príčiny).

Významným teoretickým východiskom skúmania nastolenej problematiky v odvetví obrany je ozrejmenie problému efektívnosti, resp. neefektívnosti vo verejnom sektore, teda v širšom kontexte.

1.1 EFEKTÍVNOSŤ VEREJNÉHO SEKTORA

Podľa Pekovej (2008) „efektívnosť predstavuje stav, keď sa z dostupných spoločenských zdrojov podarí získať maximálne množstvo statkov a maximálny úžitok“. V súvislosti s efektívnosťou verejného sektora daná autorka rozlišuje medzi užším a širším chápaním. V prípade užšieho chápania efektívnosti ide o tzv. paretovskú efektívnosť[1], kedy za efektívne sa považuje také riešenie, pri ktorom rastie úžitok aspoň jednému jedincovi, ale úžitok ostatných sa nemení. Širšie chápanie efektívnosti verejného sektora hovorí o výsledku vzťahu medzi veľkosťou vstupov do verejného sektora a veľkosťou výstupov z neho, pričom za vstupy možno považovať náklady a za výstupy úžitky.

Podľa Cibákovej a kol. (2012) v súkromnom sektore, kde je rozhodujúcim činiteľom zisk, je všetko podriadené dosiahnutiu optimálneho stavu medzi vstupmi v podobe nákladov a výstupmi v podobe zisku. „V súkromnom sektore si úžitok zaplatí kupujúci v cene výrobku, ktorá mu prinesie zisk. Ak existuje na trhu konkurencia, kupujúci hľadá úžitkovú hodnotu výrobku za optimálnu cenu. Výrobok však môže aj nekúpiť, ak nespĺňa očakávaný úžitok. Vo verejnom sektore musí nájsť vyjadrenie úžitku výrobca statkov, a to prostredníctvom

[1] Pozn. Podľa V. Pareta je optimálne také riešenie, pri ktorom už nemožno zvýšiť úžitok ktoréhokoľvek jednotlivca bez toho, aby sa neznížil úžitok ostatných subjektov.

vyjadrenia miery uspokojenia potrieb, ktoré majú jeho statky zabezpečiť. Robí tak preto, lebo uspokojovaním potrieb spotrebiteľov sa zároveň uchádza o poskytnutie prostriedkov z verejných rozpočtov“.

Podľa Buchtu (1997) možno vstupy vo verejnom sektore merať, a to: mzdou, podľa kategórie zamestnancov vo verejnom sektore a ďalej nákladmi, podľa ich štruktúry. Meranie výstupov je ťažšie a podľa uvedeného autora je potrebné rozlišovať:

- kvantitatívnu stránku uspokojovania potrieb (napr. v prípade vysokých škôl je to počet jej absolventov),
- kvalitatívnu stránku uspokojovania potrieb (napr. absolventi vysokých škôl s vynikajúcim prospechom).

Podľa Cibákovej a kol. (2012) podrobné štúdium literatúry ukázalo, že efektívnosť môžeme sledovať ako efektívnosť vo verejnom sektore, efektívnosť v prípade produkovaných verejných statkov, resp. poskytovaných verejných služieb (medzi ktoré patrí aj obrana) alebo efektívnosť pri hodnotení verejných projektov, resp. širšie verejných výdavkov, verejných výdavkových programov, či najširšie verejných politík[2]. Inak povedané ide o sledovanie efektívnosti vynaloženia verejných zdrojov v súvislosti s realizáciou, či zabezpečením rôznych verejných aktivít[3]. Na realizáciu verejných politík a verejných výdavkových programov sú potrebné zdroje (kľúčovou podmienkou je ich krytie finančnými zdrojmi). A keďže zdroje sú obmedzené, a teda vzácne, hľadáme pri ich alokácii také varianty, ktoré povedú k efektívnemu a účelnému nakladaniu s nimi. Na to v praxi používame ekonomické hodnotenie (evaluáciu) verejných politík a jednotlivých výdavkových programov zahŕňajúce také postupy, ktoré poskytujú informácie o ekonomicky racionálnom použití vzácnych zdrojov s ohľadom na stanovené ciele. Čo v praxi znamená, že dostupnými ekonomickými metódami preskúmame účinky verejných výdavkových programov v súvislosti s nákladmi na ich dosiahnutie.

Za predpokladu, že sa subjekty verejného sektora správajú racionálne[4], hospodária podľa zásad racionálneho ekonomického správania sa, tak potom hľadáme vzťah medzi vstupmi, výstupmi a alokačnými cieľmi. Sledujeme skutočnosť, či hodnota poskytovaných výstupov („hodnota za peniaze“ – „Value for Money“) prevyšuje náklady na ich produkciu. Zároveň je potrebné hľadať ekonomicky najprínosnejší variant s ohľadom na zvolené alokačné kritérium, napr. v rámci kritérií označovaných ako 3E, t. j. hospodárnosti – Economy, účelnosti – Efficiency a efektívnosti – Effectiveness. 3E predstavujú základné postupy, na základe ktorých hodnotíme výdavkové aktivity z hľadiska minimalizácie nákladov, nákladovej efektívnosti (resp. produktivity) a účelnosti vynaložených zdrojov s ohľadnom na stanovené ciele. Inými slovami povedané, hľadáme také riešenia, pri ktorých dosiahneme súlad medzi vyššie spomínanou ekonomickou efektívnosťou a spoločenskou efektivitou/prosperitou, ktorou rozumieme najlepšie dostupné využitie spoločenských zdrojov. V kontexte obrany tak ide o riešenie dilemy, resp. voľby medzi produkciou vojenských statkov a civilných statkov (napr. delá verzus maslo), resp. obrannej výroby verzus civilnej výroby a následne o problém efektívnosti výdavkov na obranu. Konečná voľba je výslednicou mnohých pôsobiacich

[2] Pozn. Verejné politiky sú prepojené s verejnými výdavkovými programami, v tom zmysle, že na realizáciu cieľov verejných politík využívame, resp. realizujeme rôzne verejné výdavkové programy. Na naplnenie cieľov obranno-bezpečnostnej politiky realizujeme konkrétne výdavkové programy. V zmysle Smernice ministra obrany Slovenskej republiky pre obranné plánovanie na roky 2023 až 2028 je programová štruktúra MO SR tvorená dvoma rezortnými programami (program 096 – Obrana a program 095 – Rozvoj obrany), ďalej medzirezortným programom 06E – Podpora obrany štátu a ďalšími ôsmimi medzirezortnými podprogramami, ktorých je MO SR účastníkom.

[3] Pozn. Podľa European Court of Auditors každú verejnú aktivitu možno bez ohľadu na jej povahu analyzovať ako súbor finančných, materiálnych a ľudských zdrojov uvoľnených za účelom dosiahnutia cieľov so zámerom vyriešenia určitých problémov.

[4] Pozn. Ekonomicky racionálne správanie je také, ktoré vedie najefektívnejším spôsobom a najkratšou cestou k dosiahnutiu ekonomického cieľa, z ktorého vychádzame pri správaní ekonomických subjektov.

faktorov, ktoré ju ovplyvňujú. Odborná literatúra (bližšie pozri napr.: Elias-Moreno, Bel, Sköns, Loose-Weintraub, Omitoogun, Stalenheim a i.) hovorí o bezpečnostných, politických, technologicko-priemyselných a ekonomických determinantoch. Empirické poznatky naznačujú, že v poslednej dobe práve najmä ekonomická a bezpečnostná situácia významne determinujú využitie národných zdrojov pre potreby obrany. V tejto situácii ešte viac ako inokedy do popredia záujmu vystupujú tzv. náklady obetovaných (stratených) príležitostí (tzv. trade offs costs) (Holcner a kol, 2011).

Zvýšenie efektívnosti možno podľa konkrétnych podmienok uskutočniť prostredníctvom dvoch rovnocenných variantov, a to (Kupkovič a kol., 2002):

- dosiahnutia množstva a štruktúry výstupu (napr. produkcie) pri minimálnom vynaložení zdrojov, t. j. cestou úspornosti,
- maximalizácie efektu/výstupu pri danom objeme a štruktúre zdrojov, t. j. cestou účinnosti.

Úspornosť aj účinnosť predstavujú extrémne prístupy k zvyšovaniu efektívnosti, obvykle sa prejavujú v rôznych kombináciách, pričom ich vývoj môže byť pozitívny, negatívny alebo neutrálny. Obidva extrémy vedú v podstate k rovnakým výsledkom – znižovaniu spotreby zdrojov na jednotku výstupu a tiež k zvyšovaniu produktivity práce. Efektívnosť tak nadobúda prvý hlavný charakteristický znak – hospodárnosť. Hospodárnosťou sa pritom rozumie také použitie zdrojov, kedy stanovené ciele sú splnené s čo najnižším vynaložením nákladov. Z pohľadu ekonomickej racionality a hľadania úspor to znamená dosahovať stanovené ciele s minimálnymi nákladmi (kritérium na vstupe), avšak za podmienky, že sú dosiahnuté všetky pôvodne plánované ukazovatele výstupu. Ďalej ide o účinnú transformáciu zdrojov na úžitkové hodnoty, ktorá tvorí najdôležitejšiu fázu reprodukčného procesu. Z tohto dôvodu jej teória i prax venujú najväčšiu pozornosť. A napokon ide o účinnosť uspokojovania potrieb vytvorenými úžitkovými hodnotami. Efektívnosť sa tak prejavuje vo forme účelnosti, cieľavedomosti vynakladanej práce, ktorú vyjadruje úžitková hodnota (kvalita) výstupov (výrobkov, služieb). To je druhý hlavný znak efektívnosti. Vyššie uvedené naznačuje, že ekonomická efektívnosť je veľmi zložitý jav, ktorý nemožno postihnúť jediným ukazovateľom. Preto aj analýza efektívnosti verejných výdavkov si vyžaduje existenciu vhodných ukazovateľov.

Podľa Nedbala (2007) ju možno sledovať prostredníctvom dvoch ukazovateľov, resp. v dvoch základných formách, ktorými sú:

- nákladová efektívnosť, kedy zisťujeme, aké náklady boli vynaložené na jednu naturálnu jednotku výstupu (napr. na jedného profesionálneho vojaka, na jeden kus vojenskej techniky atď.). Najefektívnejší je ten variant alternatívneho/porovnateľného výdavkového programu (projektu), ktorý má najnižšie náklady na jednu naturálnu jednotku. Daný ukazovateľ používame len vtedy, ak oceňujeme a porovnávame rovnaký typ výstupu (výstupy teda musia byť homogénne).
- produktivita verejných výdavkov, kedy zisťujeme počet jednotiek výstupu na jednu jednotku vstupu. V tejto forme definuje efektívnosť zákon o finančnej kontrole. Rozumie ňou také použitie verejných prostriedkov, ktorým sa dosiahne najvyšší možný rozsah, kvalita a prínos plnených úloh v porovnaní s objemom prostriedkov vynaložených na ich plnenie. Z uvedeného vymedzenia je zrejmé, že toto poňatie skúmania efektívnosti je založené na predpoklade benchmarkingového porovnávania výdavkových aktivít, kedy najvyššiu produktivitu má tá produkčná jednotka, ktorá z danej jednotky (fixného) rozpočtu dosiahne najviac jednotiek výstupu pri požadovanej kvalite. Takéto porovnávanie sú manažéri verejnej správy povinní zo zákona realizovať v rámci interného auditu ex post.

Viacerí autori (napr. Benčo, J., Ochrana, F.) poukazujú na to, že s určitými zvláštnosťami či už hodnotenia, alebo merania efektívnosti sa môžeme stretnúť pri verejných službách, medzi ktoré zaraďujeme aj poskytovanie čistého verejného statku v podobe obrany. V tejto súvislosti je potrebné zdôrazniť, že v službách chápeme efektívnosť v širších spoločenských súvislostiach ako pri výrobe výrobkov. Ekonomická efektívnosť aplikovaná na služobtvorné procesy (poskytovanie služieb) verejného sektora nezohľadňuje všetky aspekty a konečný efekt vynaloženej práce, čo je dané zvláštnosťami služobtvorného procesu[5].

Záverom tejto časti možno konštatovať, že efektívnosť každého javu či procesu je vždy výsledkom vzťahu medzi veľkosťou vstupov vkladaných do realizácie tohto javu či procesu, a veľkosťou výstupov, ktoré z realizácie tohto javu či procesu vychádzajú – ide teda o vzťah medzi vloženými prostriedkami (spotrebovanými vstupmi/zdrojmi vyjadrenými prostredníctvom ekonomickej kategórie nákladov) a ich ekonomickými účinkami (dosiahnutými výstupmi/výkonmi, výsledkami). Práve princíp porovnávania nákladov a výsledných efektov možno považovať za kľúčovú zásadu všade tam, kde sa hospodári so vzácnymi zdrojmi, teda aj vo sfére obrany.

1.2 PODSATATA A PRÍČINY NEEFEKTÍVNOSTI VEREJNÉHO SEKTORA

Verejný sektor, tak ako sme ho doteraz vysvetľovali, je klasifikovaný ako neziskový, lebo jeho produkcia sa nepredáva na trhu. Procesy, ktoré vo verejnom sektore existujú, a subjekty, ktoré v ňom pôsobia, sú financované väčšinou z verejných prostriedkov – verejných financií a nie sú bezprostredne závislé na dosahovaní zisku. To však neznamená, že sa majú správať neefektívne, aj keď im nehrozí bankrot a okamžitý zánik ako súkromnému sektoru. Ak je raz produkcia verejných statkov potrebná a súkromný sektor ju neponúka, treba ju zabezpečiť aj za cenu určitých ekonomických strát (Cibáková a kol., 2012), teda pomer úžitok/náklad môže byť menší ako 1, čo naznačuje, že vo verejnom sektore pripúšťame existenciu neefektívnosti.

Existuje všeobecná zhoda v názore, že pre verejný sektor je príznačná tendencia k neefektívnosti, ktorá má svoje vecné príčiny ako aj konkrétne prejavy, nazvime ich dôsledky zlyhávania verejného sektora. Podľa Buchtu (1997) vecné príčiny neefektívnosti vo verejnom sektore, podobne ako pri nedokonalostiach trhu, spočívajú v nedokonalej konkurencii, v nedokonalom toku informácií, rozdielnych záujmoch a názoroch štátnych zamestnancov a úradníkov, neobjektívnom rozhodovaní pri zadávaní zákaziek pre verejný sektor a v nedokonalosti ľudí ako hlavných aktérov rozdeľovania a využívania finančných prostriedkov. Podľa Streckovej, Malého a kol. (1998) možno za dôsledok zlyhávania verejného sektora považovať najmä: chybnú alokáciu verejných financií, menšiu inovačnú aktivitu spôsobov uspokojovania potrieb, byrokratizáciu vo fungovaní subjektov verejného sektora, ťažkopádnosť subjektov a procesov vo verejnom sektore a v neposlednom rade nerešpektovanie spotrebiteľa.

V ostatných rokoch sa v oblasti riadenia zdrojov (ľudských, materiálnych, finančných) sústreďuje pozornosť hlavne na problém neefektívnosti v spojitosti s riadením finančných zdrojov a najmä hospodárenia s nimi. Pri presadzovaní požiadavky efektívneho hospodárenia so zdrojmi sa vo verejnom sektore ako celku stretávame s množstvom problémov, spomenúť možno stav označovaný ako tzv. X-neefektívnosť[6], na ktorý už v roku 1966 upozornil americký

[5] Bližšie pozri napr. Benčo, J. Možnosti posudzovania verejného sektora. In *Efektivnost veřejného sektoru.* Sborník prací Asociace veřejné ekonomie. ESF MU Brno, 1996.

[6] Pozn.: Podľa Leibensteina sú produkčné náklady závislé nielen od použitej technológie, ale rovnako aj od úsilia organizácie znižovať náklady, resp. produkovať za danej kombinácie produkčných faktorov maximálny výstup. V tejto súvislosti vyslovil názor, že v organizáciách riadených štátom dochádza často k strate efektívnosti v dôsledku toho, že manažment nemá v oblasti nákladov motiváciu efektívne riadiť. Ak súkromná firma zníži svoje náklady o jednotku, potom sa o túto jednotku zvýši jej zisk. Ak však dôjde ku zníženiu nákladov o jednotku

ekonóm Leibenstein, H. Na druhej strane skúsenosti z praxe ukazujú, že pre obdobie uplynulých rokov sprevádzané stále silnejúcim tlakom na efektívne využívanie verejných financií, je príznačná aj výraznejšia snaha presadzovať v ekonomickom riadení subjektov verejného sektora princíp efektívnosti a s ním súvisiacej hospodárnosti a účelnosti. Dodržiavanie efektívnosti, hospodárnosti a účinnosti pri hospodárení s verejnými prostriedkami, ako aj pri iných činnostiach, ukladá orgánom verejnej správy už spomínaný Zákon č. 502/2001 o finančnej kontrole a vnútornom audite7. Napriek uvedenému, je potrebné konštatovať, že objektívne posúdenie efektívnosti vynaložených verejných výdavkov subjektov verejného sektora je v porovnaní so súkromným sektorom oveľa zložitejšie. Často si vyžaduje aplikovanie špecifických metód či postupov, príkladom ktorých sú komparatívne metódy (vrátane benchmarkingu), ale aj inputovo-outputové metódy, ďalej normy, normatívy a limity, štandardy, hodnotenie občanmi či realizovanie komplexného auditu toho ktorého subjektu a pod.

Keďže aj rezort obrany hospodári so zdrojmi, ktoré sám nevytvoril, ale mu boli pridelené v rámci jeho rozpočtu, môžeme konštatovať, že nie je hmotne zainteresovaný na spôsobe hospodárenia s týmito zdrojmi, inými slovami obrane je neraz pripisovaná tendencia k neefektívnosti ako jej vnútorná vlastnosť.

Záverom tejto časti príspevku chceme poukázať na skutočnosť, že problematike efektívnosti, resp. neefektívnosti fungovania verejného sektora a jeho správy sa v ekonomickej literatúre venujú autori už od 60. rokov 20. storočia. Rozsiahle analýzy naznačujú, že snahu optimalizovať alokáciu zdrojov a presadzovať požiadavku efektívneho hospodárenia so zdrojmi vo verejnom sektore (vrátane obrany) komplikujú viaceré skutočnosti. Za najvýznamnejšie príčiny tohto stavu možno považovať najmä existenciu byrokracie a zlyhávanie kolektívneho rozhodovania (rozpor medzi individuálnymi a spoločenskými úžitkami, obmedzenie suverenity občanov – diktátorská forma výberu, monopolné správanie sa politikov – politický cyklus).

2 EFEKTÍVNOSŤ OBRANY

Za východisko pre objasnenie problému efektívnosti v obrane sme pre potreby daného príspevku zvolili prístup českého ekonóma Ochranu, F., ktorý sleduje efektívnosť na príklade nákladového strediska, pričom berie do úvahy nákladovú efektívnosť verejných služieb. V prípade stanovenia efektívnosti vo všeobecnej rovine je jeho vzťah dvoch veličín nasledovný:

$$\text{Efektívnosť } (E) = V_i / C_i$$

kde V_i sú naturálne výstupy i-teho producenta verejnej služby a C_i sú náklady i-teho producenta verejnej služby. Efektívnosť je tak inverznou hodnotou jednotkových nákladov.

2.1 HODNOTENIE EFEKTÍVNOSTI V OBRANE

Základným subjektom ekonomického riadenia rezortu obrany, na ktorý sa plánujú a sledujú náklady a výdavky spojené s úlohami a činnosťami, ktoré zabezpečuje je nákladové stredisko. Z ekonomického hľadiska je nákladové stredisko miestom spotreby nákladov a

v organizácii verejného sektora, potom sa zníži jej celkový rozpočet o jednotku, čo následne môže byť byrokratmi považované za zníženie významu danej organizácie.

[7] Pozn.: V zmysle uvedeného zákona sa efektívnosťou rozumie maximalizovanie výsledkov činnosti vo vzťahu k disponibilným verejným prostriedkom; hospodárnosťou minimalizovanie nákladov na vykonanie činnosti alebo obstaranie tovarov, prác a služieb pri zachovaní ich primeranej úrovne a kvality; a účinnosťou vzťah medzi plánovaným výsledkom činnosti a skutočným výsledkom činnosti vzhľadom na použité verejné prostriedky.

uvádza sa pri plánovaní a účtovaní skutočných nákladov. V zmysle metodických pokynov pre programovanie v rezorte Ministerstva obrany SR (ďalej len MO SR) má nákladové stredisko vzťah k finančnému stredisku a je kmeňovým údajom modulu kontroling integrovaného informačného systému (IIS), na ktorom sa sledujú plánované a vynaložené náklady súvisiace s činnosťami, ktoré zabezpečuje (modul CO – Sledovanie a vyhodnocovanie nákladov a výnosov, napr. L10101 – 1. mechanizovaná brigáda).

MO SR používa tzv. organizačné nákladové strediská, ku ktorým sa viažu prevádzkové náklady, ktoré súvisia s činnosťou danej organizačnej zložky. A ďalej tzv. účelové nákladové strediská, ku ktorým sa viažu špecifické náklady, ktorých účel vynaloženia je potrebné sledovať samostatne. Aktuálnu štruktúru nákladových stredísk rezortu MO SR, ako aj ich priradenie ku konkrétnym úlohám a podúlohám vymedzuje metodický pokyn pre programovanie na aktuálny programovací 6-ročný cyklus (konkrétne jeho príloha č. 3). V súlade so strednodobým predurčením nákladových stredísk na plnenie úloh sú tieto primárne priradené k jednej úlohe a podúlohe, resp. k ďalším úlohám, na ktorých plnení sa dané nákladové stredisko podieľa. Štruktúra nákladových stredísk a ich priradenie k úlohám a podúlohám obsiahnutá v metodických pokynoch pre programovanie nadväzuje na predchádzajúci programovací cyklus a obsahuje všetky pripravované a schválené reorganizačné zmeny ku dňu schválenia daného metodického pokynu. Ak vznikne potreba priradenia operačnej úlohy/podúlohy k nákladovému stredisku, ktorá nie je obsiahnutá v danom metodickom pokyne, predloží príslušné nákladové stredisko svoju požiadavku manažérovi podprogramu. Po jej schválení a predložení na Sekciu obrannej politiky MO SR, poverený pracovník sekcie doplní požiadavku aj do využívaného integrovaného informačného systému.

Nákladové stredisko možno vnímať ako produkčný systém, v ktorom sa prostredníctvom transformačného procesu menia vstupy na výstupy. Práve v objektívnom zhodnotení fungovania jednotlivých nákladových stredísk rezortu MO možno vidieť aj určité východisko pre posudzovanie jeho ekonomickej efektívnosti, resp. konkrétnejšie pre hľadanie a dosahovanie „vnútorných“ úspor vo výdavkoch na obranu.

2.2 EKONOMICKÁ EFEKTÍVNOSŤ VÝDAVKOV NA OBRANU

Posudzovať ekonomickú efektívnosť verejného sektora, resp. jeho jednotlivých subjektov je značne zložité. Najčastejšie sa spája s efektívnosťou verejných výdavkov, ale aj tam sú výstupy ťažko kvantifikovateľné. Vieme napr. vyčísliť náklady na výstavbu jedného kilometra diaľnic, ale výstup v podobe spokojnosti vodičov môžeme vyčísliť len sprostredkovane, napr. cez zakúpenú diaľničnú známku. Niet sporu o tom, že z hľadiska objemu vynaložených zdrojov (z pohľadu jednotlivých štátov, zoskupení, resp. celosvetovo) možno obranu a bezpečnosť považovať za jedny z najdrahších komodít tohto storočia. A to je významný dôvod pre zefektívnenie obranných výdavkov, resp. širšie pre objektivizáciu verejných výdavkov.

Problém efektívnosti výdavkov na obranu veľmi úzko súvisí s hľadaním odpovedí na dve kľúčové otázky. Prvá otázka, ktorú si kladú najmä politici, bezpečnostní aktéri a ekonómovia znie: Koľko obrany skutočne potrebujeme? Inými slovami, v zmysle prístupu Ochranu, F., aký má byť objem naturálnych výstupov (hodnota Vi). Pozornosť sa následne sústreďuje na problém efektívneho množstva obrany. V zmysle ekonomickej teórie efektívne množstvo verejného statku vzniká za rovnováhy, ktorá odráža rovnosť medzi súčtom marginálnych (hraničných) úžitkov a marginálnych (hraničných) nákladov[8]. „Efektívne

[8] Pozn. Marginálny (hraničný) je pojem, ktorým sa rozumie dodatočná jednotka príslušnej veličiny. Hraničný (marginálny) úžitok/užitočnosť je prírastok užitočnosti vyvolaný spotrebou dodatočnej jednotky daného statku. Hraničné (marginálne) náklady predstavujú prírastok celkových nákladov v dôsledku zvýšenia výroby, či produkcie statku o 1 jednotku.

množstvo verejného statku, ktoré maximalizuje spoločenský blahobyt je v bode, kde sa suma hraničných hodnotení všetkých jednotlivcov rovná hraničným nákladom na produkciu poslednej jednotky verejného statku“ (Ochrana, 2001).

V súvislosti s obranou je však potrebné zdôrazniť viaceré fakty. S pridaním ďalšieho spotrebiteľa (občana), resp. so spotrebou každého ďalšieho občana sú späté nulové marginálne náklady. Obrana ako čistý verejný/kolektívny statok prináša úžitok celej spoločnosti (štátu), ale aj každému jej jednotlivému občanovi, pričom spotreba tohto statku jedným občanom nevedie k zníženiu úžitku zo spotreby ďalšími občanmi. Ak sa teda usilujeme o vymedzenie efektívnosti obrany z pohľadu občana, tak možno hovoriť o vzťahu, resp. pomere medzi očakávaným dosahovaným úžitkom pre občana a nákladmi vynaloženými na dosiahnutie tohto úžitku, resp. štandardizovanej kvality. Ďalším špecifikom obrany je tiež skutočnosť, že jednotlivci (občania) ako užívatelia statkov nesignalizujú mieru úžitku, ktorá im z jeho spotreby plynie. V súkromnom sektore si úžitok zaplatí kupujúci v cene výrobku, ktorá predávajúcemu prinesie zisk. Ak na trhu existuje konkurencia, kupujúci hľadá úžitkovú hodnotu výrobku za optimálnu cenu. Ak výrobok nesplní očakávaný úžitok, môže ho aj nekúpiť. Ako sme už uviedli vyššie, vo verejnom sektore však musí nájsť vyjadrenie poskytovaného úžitku samotný producent statkov a služieb (v prípade obrany teda OS SR ako rozhodujúci výkonný prvok systému obrany Slovenskej republiky), a to prostredníctvom vyjadrenia miery uspokojenia potrieb, ktoré majú jeho statky zabezpečiť. Robí tak preto, lebo uspokojovaním potrieb spotrebiteľov (občanov) sa zároveň uchádza o poskytovanie prostriedkov z verejných rozpočtov.

Problém efektívneho množstva obrany je teda spätý aj s problémom efektívnej ponuky obrany (resp. širšie verejných statkov). Podľa Ochranu (2011) poskytovanie (čistých kolektívnych) verejných statkov je efektívne vtedy, keď sa súčet hraničných mier substitúcie všetkých spotrebiteľov (občanov) rovná hraničnej miere transformácie. Podmienkou efektívnosti je, aby sa celkové množstvo súkromných statkov, ktorých sú spotrebitelia ochotní sa vzdať (súčet hraničných mier substitúcie), rovnalo množstvu, o ktoré sa výroba skutočne zníži (hraničná miera transformácie).

Druhou otázkou, na ktorú dlhodobo hľadáme odpoveď je otázka: Koľko zdrojov (peňazí) je potrebné vynaložiť na zabezpečenie potreby národnej obrany?, čo ekonómovia často vyjadrujú anglickou vetou: How much is enough? V tejto súvislosti je potrebné spomenúť meno Robert S. McNamara9, ktoré je v histórii verejných financií neodmysliteľne spojené s metódou riadenia alokácie verejných výdavkov určených na zaistenie verejných statkov a služieb, známou pod označením Planning, Programming and Budgeting System (PPBS), ktorá predstavuje základný princíp kontroly verejných prostriedkov prideľovaných rozhodnutím politikov pre potrebu inštitúcií verejného sektora uspokojujúcich dopyt po verejných statkoch a službách (Pernica, 2008). Pre súčasné európske chápanie je pomerne prekvapivé vtedajšie zistenie McNamaru a jeho tímu, že v prípade financovania verejného výdavkového programu neexistuje niečo ako je „optimálne percento“ HNP, resp. HDP vydávané na ten či onen výdavkový program. Ak má byť dosiahnutá efektívnosť výdavkov, potom by štátne inštitúcie, a najmä armáda, či ozbrojené sily mali postupovať podľa podobných pravidiel hodnotenia investícií, tak ako to robia súkromnoprávne inštitúcie. Základnú inšpiráciu pri hľadaní inovácií v systéme riadenia výdavkového programu obrany, ktoré by umožňovali lepšiu kontrolu tohto programu a väčšiu efektívnosť vojenských výdavkov, resp. širšie zefektívnenie výdavkov vynakladaných v odvetví obrany tak nachádzame v spomínanej knihe v podobe aplikácie

[9] Pozn. McNamara – bývalý minister obrany USA v Kennedyho, Johnsonovej i Nixonovej administratíve, neskôr prezident Svetovej banky. Niekoľko rokov sa spoločne so svojím tímom pokúšal odpovedať americkej verejnosti na otázku: „Koľko je v skutočnosti potrebných peňazí pre potreby národnej obrany USA?“ Problémy, s ktorými sa so svojím tímom stretával pri hľadaní ekonomicky racionálnych odpovedí na túto otázku obsiahli jeho dvaja spolupracovníci v knihe s názvom How Much is Enough? *Shaping the Defense Program, 1961-1969* vydanej v roku 1969.

nasledovných pravidiel pre investičné rozhodovanie známe z komerčnej sféry (Enthoven, Smith, 2005): „Najskôr nájdi adekvátny počet komplexných variantov zabezpečenia úloh ozbrojených síl, a potom vyber variant s čo najvyššou ekonomickou efektívnosťou vynaložených zdrojov. K tomu všetkému si však prispôsob systém riadenia, aby si riadil ty, a v žiadnom prípade nie len súhlasil alebo nesúhlasil s predkladanými riešeniami. Následne presvedč svojich spolupracovníkov o tom, že podstata riešenia tzv. rýdzo vojenských problémov má ekonomický základ“.

Pokiaľ budeme brať do úvahy obranné výdavky, ktoré si spoločnosť môže dovoliť minúť, platí, že budú neefektívne, pokiaľ ich veľkosť bude väčšia ako úžitok, ktorý poskytujú. V tejto súvislosti je tiež potrebné zdôrazniť, že odvodzovanie výdavkového stropu z komparácie s najlepším alebo s priemerom porovnateľných krajín neznamená, že dosiahneme rovnaký výsledok. Naopak môže to viesť k vysokej neefektívnosti vyčleňovaných prostriedkov. V tomto ohľade by mali byť vždy formulované vlastné alternatívne projekty, vypočítaná ich efektívnosť, a až následne má byť vyjednávané s politikmi o prostriedkoch na ich krytie (Pernica, 2008).

V súvislosti s vyššie uvedeným považujeme za potrebné konštatovať, že MO SR musí aplikovať procesy, ktorými zaistí čo najefektívnejšie a najhospodárnejšie využitie verejných zdrojov. To znamená, že je potrebné využívať opatrenia, ktoré umožňujú balansovať medzi nárokmi na čo najvyššiu operačnú efektivitu pri plnení úloh rezortu a prijateľnými nákladmi na jej zabezpečenie. Pozitívnym krokom k naplneniu uvedeného cieľa môže byť prijatie dokumentu „Metodika hodnotenia investícií v rezorte Ministerstva obrany Slovenskej republiky“ (2021), ktorý by mal byť implementovaný do praxe rezortu s cieľom: „...predstaviť súbor pravidiel určených pre hodnotenie investícií v podmienkach rezortu obrany. Hodnotením investície sa rozumie systematický proces, ktorý je zameraný na jasné definovanie požiadavky, na uvažovanie o rôznych spôsoboch realizácie požiadavky, na odhadovanie a posudzovanie nákladov, prínosov a rizík každého z potenciálne užitočných riešení, vrátane ich prehľadného prezentovania. Výsledok hodnotenia investície poskytuje odporúčanie pre orgány, ktoré prijímajú rozhodnutia. Využitie verejných zdrojov by malo byť dôsledne obhájiteľné a založené na overiteľných údajoch, aby rozhodujúce orgány mohli prijímať informované rozhodnutie“.

Keďže rozhodujúcim výkonným prvkom systému obrany štátu je jeho armáda, resp. v prípade Slovenskej republiky ozbrojené sily, je potrebné v rámci skúmanej problematiky venovať náležitú pozornosť aj otázke vojensko-ekonomickej efektívnosti (uplatníme teda mikroekonomický pohľad na danú problematiku), ktorá by mala predstavovať kľúčovú zásadu riadenia všetkých vojenských činností. Podstata zisťovania vojensko-ekonomickej efektívnosti (EV) spočíva opäť v princípe obsiahnutom vo všeobecnej teórii ekonomickej efektívnosti, konkrétne v posudzovaní vzájomného pomeru medzi cieľovým užitočným efektom vojenskej činnosti (resp. posudzovaných variantov) a spoločenskými nákladmi, ktoré je nutné vynaložiť na ich dosiahnutie.

Záverom tejto časti príspevku považujeme za potrebné poukázať najmä na potrebu interného, čiže operatívneho zvyšovania efektívnosti v rezorte MO, ktoré je odborníkmi považované za pružnejšie a systémovejšie riešenie ako vládne nariadenia alebo nespokojnosť verejnosti.

ZÁVERY A ODPORÚČANIA

Efektívnosť verejného sektora je podľa odborníkov (Strecková, Malý, 1998) podporovaná viacerými nástrojmi. Inými slovami, pre dosiahnutie efektívneho stavu musia byť v danom odvetví splnené podmienky efektívnosti (vonkajšie – politické usporiadanie spoločnosti, fungujúci trhový sektor; vnútorné – konkurenčné prostredie vo vnútri verejného sektora, financovanie verejného sektora podľa jeho úžitkov a výkonov, verejná kontrola,

schopnosť dostatočne jasne formulovať ciele organizácie alebo odvetvia verejného sektora) a zároveň uplatňované faktory efektívnosti (veda a technika, znalosť štruktúry všetkých činností, uplatňovanie všetkých foriem deľby práce, kvalifikácia a iniciatíva pracovníkov a v neposlednom rade systém riadenia). Keďže práve od systému riadenia závisí spôsob a intenzita využívania všetkých ostatných faktorov efektívnosti, práve tento možno považovať za najvýznamnejší, a preto je potrebné venovať mu náležitú pozornosť.

Organizácia, či už súkromná alebo verejná, ktorá je orientovaná na dosiahnutie maximálneho výkonu, nemôže byť nikdy úplne spokojná s dosiahnutým stavom svojho rozvoja, nastavením svojich vnútorných procesov a spôsobom ich realizácie. Organizácie musia sústavne hľadať cesty a realizovať racionalizačné opatrenia za účelom lepšieho naplánovania svojho poslania a vytvárania vyššej úžitkovej hodnoty pre svojich zákazníkov (občanov). Pojem „lepší“ vyjadruje jednak efektívne, účelné a transparentné využitie všetkých aktív (zdrojov, potenciálu) organizácie, ale tiež znižovanie nákladov na všetky jej uskutočňované činnosti (hospodárnosť). V procese strategického riadenia tak hovoríme o potrebe permanentnej adaptácie organizácie. Tento imperatív sa dotýka samozrejme aj fungovania administratívy štátu a zaisťovania verejných statkov spoločnosti, vrátane obrany a bezpečnosti. Práve zaistenie obrany štátu predstavuje špecifickú oblasť, ktorá sa nezaobíde bez systematického a nepretržitého prispôsobovania sa novým výzvam. Zmyslom prispôsobovania systému obrany štátu a bezpečnostného systému nie je na rozdiel od podnikovej sféry získanie konkurenčnej prevahy na trhu, ale zaistenie vierohodnej úrovne obrany a bezpečnosti a vytvorenie predpokladov (obranyschopnosti) pre účinné pôsobenie všetkých nástrojov pri plnení daných úloh. Skúsenosti z praxe ukazujú, že moderné štáty aplikujú prístupy najlepšej praxe, ktoré vytvárajú predpoklady pre efektívne, účelné, hospodárne a transparentné vytváranie vojensky relevantného, vierohodného a zdrojovo udržateľného potenciálu determinujúceho ich obranyschopnosť a bezpečnosť (Procházka, Nečas, 2020).

Rezort obrany, ktorý je ako súčasť verejného sektora pod tlakom vonkajších faktorov efektívnosti, je sám nútený nachádzať a uplatňovať sústavu vnútorných faktorov efektívnosti, pričom úsilie by malo byť sústredené najmä na zdokonaľovanie systému riadenia (napr. v zmysle dôsledného uplatňovania princípu zodpovednosti vedenia za vážnejšie poruchy rezortu), deľby práce a štruktúry všetkých činností, ktoré sa v rámci rezortu realizujú; skvalitnenie činnosti MO SR v oblasti riadenia obrany štátu a riadenia, výstavby a kontroly OS SR; racionalizáciu štruktúr a optimalizáciou vnútorných procesov MO SR a OS SR; intenzívnejšie využívanie vedy a techniky; a v neposlednom rade podnecovanie iniciatívy a zvyšovanie kvalifikácie zamestnancov a lepšie využitie ich potenciálu.

Veríme, že poznatky prezentované v danom príspevku môžu prispieť nielen k efektívnejšiemu využívaniu disponibilných (najmä finančných) zdrojov a zlepšovaniu výsledkov v odvetví obrany, ale aj efektívnejšiemu fungovaniu celého verejného sektora na Slovensku. Zároveň môžu byť podnetom či zdrojom inšpirácií k realizácii ďalšieho skúmania a šírenia poznatkov z danej problematiky v budúcnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BUCHTA, M. Faktory a hodnocení efektivnosti ve veřejném sektoru se zaměřením na vysoké školy a armádu. In *Efektivnost veřejného sektoru.* Sborník prací Asociace veřejné ekonomie. ESF MU Brno, 1997, 226 s. ISBN 80-210-1486-5.

ELIAS-MORENO F., BEL G. *Institutional Determinants Of Military Spending.* [online]. [cit.2022-6-28]. Dostupné na: <www.ub.edu/irea/working_papers/2009/200922.pdf/>.

ENTHOVEN, A. C., SMITH, K. W. *How Much is Enough? Shaping the Defense Program, 1961-1969.* Reprint of the 1st ed. Santa Monica : RAND, 2005, ISBN 0-8330-3826-5.

HOLCNER, V., OLEJNÍČEK, A., HORÁK, R., MUSIL, P. 2011. *Základy ekonomiky obrany státu.* Brno : UNOB, 2011, 135 s. ISBN 978-80-7231-817-9.

KUPKOVIČ, M. a kol. *Podnikové hospodárstvo.* Bratislava : Sprint vfra, 2002, ISBN 80-88848-93-8

Metodika hodnotenia investícií v rezorte Ministerstva obrany Slovenskej republiky. Analytický útvar MO SR, 2021.

NEDBAL, J. Racionální hospodáření se zdroji ve sféře obrany – obecný pohled. In *Vojenské rozhledy.* ISSN 1210-3292, 2007, roč. 16, Zvláštne číslo: Ekonomická teorie a obrana, s. 131-138.

NEMEC, J. a kol. *Verejné financie.* Bratislava : Sprint, 2011, 640 s. ISBN 978-80-8939-46-6.

OCHRANA, F. *Veřejný sektor a efektivní rozhodování.* Praha : Management Press, 2001, 246 s. ISBN 80-7261-018-X.

PEKOVÁ, J. *Veřejné finance, úvod do problematiky.* 4. vyd. Praha : ASPI, 2008, 579 s. ISBN 978-80-7357-358-4.

PERNICA, B. Kolik je skutečne třeba (peněz pro potřeby národní obrany)? In *Vojenské rozhledy.* ISSN 1210-3292, 2008, roč. 17, č. 2, s. 196-199.

PROCHÁZKA, J., NEČAS, P. *Přístupy k tvorbě bezpečnostních a obranných strategií.* Banská Bystrica : Belanium. Vydavateľstvo UMB, 2020, 202 s. ISBN: 978-80-557-1656-5.

SKÖNS E., LOOSE-WEINTRAUB E., OMITOOGUN W., STÅLENHEIM P. *Military Expenditure (Chapter* 6) In SIPRI YEAR BOOK 2002 [online]. [cit.2022-06-28] Dostupné na: <http://www.sipri.org/yearbook/2002/files/SIPRIYB0206.pdf/>.

Smernica ministra obrany Slovenskej republiky pre obranné plánovanie na roky 2023 až 2028. Bratislava : MO SR, 2021, Č. p.: SEOP-42-9/2021.

STRECKOVÁ, Y., MALÝ, I. a kol. *Veřejná ekonomie pro školu i praxi.* Praha : Computer Press, 1998, 214 s. ISBN 80-722-61-126

VORLÍČEK, J. *Úvod do ekonomie veřejného sektora.* Praha : VŠE, Oeconomica, 2008, 384 s. ISBN 978-80-245-1419-2.

Zákon č. 502/2001 Z.z. o finančnej kontrole a vnútornom audite a o zmene a doplnení niektorých zákonov. [online]. [cit. 2022-09-06]. Dostupné na internete: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/502/20120301.html>.

Ing. Viera FRIANOVÁ, PhD.
Katedra logistického zabezpečenia, Akadémia ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši, Demänová 393, 031 01 Liptovský Mikuláš
viera.frianova@aos.sk

KATEGORIZÁCIA BEZPEČNOSTNÝCH HROZIEB AKO INDIKÁTOR STAVU MEDZINÁRODNEJ BEZPEČNOSTI

CATEGORIZATION OF SECURITY THREATS AS AN INDICATOR OF THE STATE OF INTERNATIONAL SECURITY

Veronika GAŠKOVÁ

ABSTRACT

By threat, also in the sense of security threat, we understand the dependence between unexpected, dangerous social and natural phenomena and the status of the time, which has a built-in structure of protection through various systems with different scope. The analysis is focused on threats that can trigger various conflicts or wars at various levels. It has two parts, while the first focuses on definitions of types of threats through selected theories. The second describes threats in specific cases, the reasons for their occurrence as well as triggering mechanisms.

Keywords: security, threat, migration, environment, religion

ÚVOD

Teoretický rámec štúdie vychádza zo súčasne platných pravidiel vedeckého výskumu venovanému oblasti bezpečnosti. Konkretizuje sa prostredníctvom analýzy hrozieb, najmä tých, ktoré môžu byť súčasným aj budúcim spúšťačom vojen, vojenských a politických konfliktov na rôznych geopolitických úrovniach.

Analýza má dve polohy, prvá je metodologická a klasifikačná. Spracúva podnety a výsledky zaužívaných definícií typov hrozieb (od národných po globálne) prostredníctvom viacerých vybraných teórií. Druhá poloha je mapovanie – použitá na ilustráciu ako sa tieto hrozby rôznej úrovne materializujú v konkrétnych prípadoch, prečo vznikajú, ktoré spúšťacie mechanizmy ich predurčujú, ale aj zhoršujú či eliminujú.

Za dôležitú časť analýzy je potrebné považovať aj hodnotenie vnútroštátnych i medzinárodných udalostí, ktoré spôsobujú zmenu v hierarchii hrozieb, ak napr. národné či kontinentálne prerastajú do globálnych. Priestor je venovaný aj problému, prečo je to v niektorých prípadoch trvalý jav a kedy je možná jeho eliminácia.

Časťou analýzy je aj stručná charakteristika prostriedkov, akými sa hrozby riešia, ako príklad je vybraná environmentálna bezpečnosť. Cieľom predmetnej analýzy je teda porovnanie problematiky hrozieb v čase a priestore – od starovekého Grécka až po súčasnosť v globálnom geografickom priestore pri vybraných udalostiach.

Hlavnou výskumnou metódou je komparácia, ďalej historická analýza/syntéza. Za podstatnú časť metodologického spracovania považujeme aj hermeneutickú metódu, keď sa skúmajú vnútorné príčiny sledovaných udalostí.

1 KLASIFIKÁCIA HROZIEB – ŠIRŠÍ ANALYTICKÝ RÁMEC

Hrozba aj vo význame bezpečnostná hrozba je autentický termín pre vyjadrenie závislosti medzi neočakávanými, nebezpečnými spoločenskými i prírodnými javmi a

statusom doby, ktorá má vybudovanú štruktúru ochrany prostredníctvom rôznych spoločenských, politických, ekonomických, vojenských a najmä axiologických systémov s trvalou, alebo časovo a geograficky vymedzenou pôsobnosťou.

Zmienenú závislosť teda okrem materiálno - technických podmienok predurčujú najmä špecifické nemateriálne podmienky, akými sú vyššie zmienený politický systém, ale aj iné ideové koncepty, akými sú náboženstvo, zdieľaná národná, rasová i kultúrna identita.

Najviac sa pri modelovaní závislosti uplatňujú rôzne filozofické systémy a ich interpretácie. Od staroveku sú to koncepty **Heraklita, Aristotela, Thukytida**. V priebehu storočí počas I. a II. tisícročia poznáme širokú škálu konceptov závislosti hrozieb od existencie a trvalosti spoločenských systémov, ktoré sú už budované na špecifických paradigmách a teóriách.

Aby sme spomenuli aspoň niektoré novoveké, treba spomenúť najmä tie, ktoré sú založené na exaktných vedeckých metódach, formulovaných vďaka rozvoju prírodných a spoločenských vied. Ale aj v tomto prípade časového určenia už platia rôzne orientované koncepty založené na rôznorodých vedeckých prístupoch (i metódach):

- štrukturálno - dynamické aspekty prístupov, kde skutočná závislosť hrozieb od spoločenského vývoja je daná štrukturálno - dynamickým prístupom, napr. teórie **I. Newtona, D. Huma,** neskôr **R. Descartesa**, ale aj **I. Kanta** a **G. F. Hegela**;
- dialekticko - materialistické aspekty prístupov, budované na základe jednoty a boja protikladov v prírode i spoločnosti, ktoré nemožno natrvalo absolutizovať do nemennej podoby, ale podliehajú zmenám najmä na základe nových vedeckých výskumov. Sú to napr. **Marxove** a vôbec marxisticky orientované typy hrozieb, ktoré sa stávajú akýmsi kritickým syntetizátorom zmien i konania vyúsťujúceho do nových teórií a paradigiem;
- najnovší výskum (myslíme tým výskum v 20. storočí) hrozby vníma v zásade tiež dialekticky, aj keď táto dialektika je označovaná ako existencializmus (dialektika subjektivizmu), štrukturalizmu (dialektika štruktúry v spoločnosti, ale aj dialektika metód výskumu v exaktných vedách, najmä v matematike/geometrii, fyzike, astronómii).

V prvom prípade môžeme napríklad uviesť **J. P. Sartra**, v druhom prípade teórie zastúpené najmä Kodanskou školou a v treťom je pozoruhodná tzv. Švajčiarska dialektická škola reprezentovaná vedcami **G. Goentshomom** a **E. Bernaysom** (Goentshom, Bernays, 1986).

Na prelome 20. a 21. storočia ešte v bezpečnostných teóriách rezonovalo ponímanie hrozieb v súvislosti s delením bezpečnosti na vojenskú a nevojenskú, kde tiež platila závislosť medzi neočakávanými (hrozbami) a inými udalosťami ohrozujúcimi mier a stabilitu, bola však inak definovaná a klasifikovaná na základe stupňa rizika a ohrozenia[1] (Lasicová, Ušiak, 2013).

Z uvedeného textu môžeme hrozby analyzovať rôznym spôsobom, v podstate na základe historického konsenzu, na základe filozofických konceptov, nových objavov vo vede a výskume na základe relevantných politických zmien v lokálnom i globálnom meradle. V podstate však platí, že čo je podstatné v teórii bytia (ontológii), nemusí byť platné v teórii poznania (gnozeológii) a táto formula bola aj základom delenia bezpečnosti na vojenskú a nevojenskú, samozrejme s určitými špecifikami (Lasicová, Ušiak, 2013).

Inú, pozoruhodnú klasifikáciu hrozieb uvádza poľský autor **L. F. Korzeniowski**. Hrozba je podľa neho termín, ktorý závisí od charakterizovanej situácie a zdroja deštrukcie. Možno ich deliť na:

[1]Termíny riziko, ohrozenie, hrozba sa v odbornej literatúre rozlišovali na základe intenzity príčin a účinkov (pozn. autorky).

- hrozby objektívne/subjektívne;
- hrozby vnútorné/vonkajšie;
- hrozby individuálne/skupinové;
- hrozby abstraktné/konkrétne;
- hrozby potenciálne/aktuálne;
- hrozby hodnotovo konštruktívne/deštruktívne;
- situácia statická/dynamická (Korzeniowski, 2008, s. 184).

O charaktere, diferenciáciách i podobnosti účinku na spoločenstvo existujú teda viaceré názorové prúdy. Súvisia najmä s tým, akým spôsobom sa bude rozvíjať teória o bezpečnosti – bezpečnostná veda – sekuritológia. Približne jednu dekádu už trvá diskusia o názve vednej disciplíny, ktorá sa zaoberá špecifikami bezpečnosti ako takej.

V rámci diskusie vznikli a pretrvávajú najmä dva názorové prúdy. Prvý zastáva názor, že „bezpečnostnú vedu“ (ak použijeme jeden z uvedených názvov) nie je potrebné budovať ako samostatný vedný odbor, že je súčasťou už etablovaných spoločenských vied. Druhý názor vypovedá o tom, že „bezpečnostná veda“ je už svojim zameraním, štruktúrou a rozsahom problematiky typickým interdisciplinárnym odborom, pretože jeho komplexnosť možno využiť pri začleňovaní do jej štruktúr aj z iných vedných odborov a ich špecifických metód.

Diskusia, zdá sa, má priebehový, ale v podstate trvalý charakter, čím sa len potvrdzuje názor o tom, čo bolo v úvode spomínané z hľadiska terminologických problémov. Je to teda súvislosť, ktorá je zjavná.

Aby sme prispeli k problematike, uvedieme iný príklad z vedeckej oblasti. Týka sa vedného odboru kulturológia, vznik ktorého zaznamenávame okolo 70. rokov 20. storočia. Okolo názvu tejto disciplíny prebiehali takmer totožné polemiky, či to budú kultúrne štúdie, kulturológia, alebo kultúrne dimenzie politológie (Jaurová, 2013). Citovaná autorka sa zaoberá práve tým, či si kultúrne dimenzie politiky môžu vystačiť s kultúrou vnímanou len ako eseje, alebo je potrebná vedecká dimenzia formou samostatného vedného odboru. V každom prípade sa vedný odbor kulturológia ujal a stal sa študijným odborom na viacerých slovenských i zahraničných vysokých školách i univerzitách.

Práve v súvislosti s touto diskusiou nad vedným odborom môžeme potvrdiť, že skúmanie bezpečnosti a špecifických hrozieb musí obsahovať aj tento aspekt, ktorý sa zaoberá kulturológia, aj keď to na prvý pohľad nie je zjavné. Pretože každá hrozba v histórii, od najstarších záznamov až po súčasnosť, mala aj kultúru ako istý spúšťač, verifikačný, iniciačný, alebo naopak, ako integračný prvok v priebehu a výsledku hrozby.

Aby sme mohli uzavrieť túto časť predloženej štúdie o definovaní hrozby ako takej, je potrebné okrem uvedených konotačných spojitostí uviesť ešte dôležité – v podstate priestorové aspekty hrozieb, ktoré nie sú dostatočne teoreticky rozpracované preto, že neboli historicky trvalo určené ako globálne, alebo priestorovo inak definované. Nemali súvislosť s klasifikáciou uvedenou autorom **Korzeniowskim**.

Z hľadiska sémantického a lingvistického úzusu budeme však podľa teoretických zvyklostí krátko definovať nasledovné pojmy, ktoré môžu pomôcť objasniť, čím bola predurčená veľmi dôležitá priestorová rozloha hrozieb.

1. Kanonizácia sily (moci) od stredoveku po súčasnosť

Je to globálny aspekt sila/moc existovala vždy ako jedno z hlavných kritérií vzniku a pretrvávania hrozby. Nie je rozhodujúce, či „globálny“ aspekt v staroveku, stredoveku aj súčasnosti zahŕňal priestory rôznej veľkosti a konglomerácie. Aj keď sa nepoužívalo toto spojenie, slovo *global* malo vždy význam ako určitý známy, veľký, poznateľný a dosiahnuteľný svet. Len rozloha sa menila v súvislosti so zemepisnými objavmi. Zároveň

kanonizácia sily/moci znamenala nutnosť zbrojenia v štátoch/ríšach, ktoré spolu susedili, alebo boli vo vzájomnej sfére. V závislosti od tohto faktu boli už naši predkovia alergickí na nerovnosť. Preto poznateľný, dosiahnuteľný svet považovali za využiteľný aj pre svoje spoločenstvo. Nebolo rozhodujúce (a spočiatku na to ani neboli prostriedky), či tento svet má rozlohu ríše, malého územia, alebo bol určovaný inými kvalitami, napr. dostatkom vody a splavnými riekami.

Kanonizácia moci a jej rozdelenie medzi záujmovými spoločenstvami však bolo vždy dočasné. Vedci v tomto zmysle hovoria o výkonnej nerovnosti *(achievement based inequality)* (Bregman, 2020, s. 114).

2. Participácia funkčných vzťahov

Geopolitika tiež predurčuje priestorovú rozlohu hrozieb. Geopolitika ako systém usporiadania sveta má cieľ sformovať vzťahy medzi časťami (štátmi, ríšami) a celkom (naša planéta Zem). Ak časti a celok chcú natrvalo participovať na vzájomných funkčných vzťahoch, musí geopolitika obsahovať navzájom zviazané a rešpektované entity z vedy (politika, ekonómia, demografia, sociálna politika, kultúrna politika, atď.), ako aj rozhodovania, ktoré tieto entity riadia a možno ich vyjadriť dvoma termínmi navzájom dôsledne sa rešpektujúcimi *démos* a *kratos* (ľud a vláda). Ak nie sú obsahovo či vzťahovo rešpektované, či už vedou alebo vzťahom ľud a vláda, geopolitika začína formovať hrozby (Cygankov, 2003).

3. Morálne konotácie

Morálne konotácie tiež predurčujú priestorovú rozlohu hrozieb. Morálne diskrepancie v spoločnosti boli a sú súčasťou vzniku, nárastu a pretrvávania globálnych hrozieb.

Jeden z významných renesančných autorov **N. Machiavelli** vo svojom diele Vladár obhajuje primát politiky pred mravnosťou a náboženstvom. Pripisuje sa mu právom termín *machiavelizmus*, politika uskutočňovaná bez ohľadu na prostriedky, akými sa dostala k cieľu. Dnes, z hľadiska humanistickej morálky, sa tento typ politiky vníma ako vážna hrozba. V histórii existuje množstvo príkladov na tento negativistický vzťah, stačí keď spomenieme rasizmus, fašizmus, terorizmus, fundamentalizmus a i., pretože všetky uvedené mali a majú v podstate globálne ambície tým viac, že dnes je možné globalizovať hrozby týkajúce sa negativizmu k morálke ako takej, ktorá by mala byť základom liberálnej spoločnosti prostredníctvom informačných technológií (Marenčinová, 2019).

Jedna z najaktuálnejších globálnych hrozieb súčasnosti sa spája s environmentálnymi problémami. Je spracovaná nielen mnohými vednými odbormi, ale aj rôznorodými mediálnymi kampaňami a má trvalé miesto v protestných aktivitách rôznych občianskych združení na celom svete. Dôvodom je oneskorené uvedomenie, že ľudstvo nie dosť rýchlo a systematicky vníma ako vážnu hrozbu medzigeneračné dopady tejto nedôslednosti. Budúce generácie budú trvalo splácať životnému prostrediu dlhy za túto nedôslednosť.

Pre vedcov i laikov je však zaujímavý názor na túto problematiku, ktorý nájdeme už v predsokratovskej filozofii, napr. u **Parmenida** (540 – 470 p.n.l.). Zo zachovalých Parmidových zlomkov sa nedá odvodiť, ako dospel k svojmu chápaniu bytia, ale podstatou je pojem *ultimo* alebo *ultimi*, čo znamená hľadať príčinu vzniku sveta ako prvý úkaz; ako druhý úkaz, alebo súčasť tejto príčiny, je definovaná sebestačnosť, ako logicky nutný základ všetkého, čo bolo náhodne stvorené. A práve túto sebestačnosť je potrebné podľa **Parmenida** (ale aj podľa iných predsokratikov a eleatov) chrániť, aby jej kontúry zostali v rovnováhe. Toto zachovanie rovnováhy prírody je dôležitým oddelením reality od mytológie v európskej kultúre, ale pravdepodobne sa tieto názory podľa bádateľov v tejto oblasti objavili aj vo védskej a budhistickej tradícii (Kolakowski, 1999, s. 38).

Potreba sebestačnosti – preložené do súčasnej terminológie – zabezpečenie ekologickej rovnováhy a ochrana environmentu, je dnes ohrozená takým spôsobom, aký história nepozná. Nerovnomernosť v príčinách zmien životného prostredia a ich dôsledkov podporuje formulovanie rozhodujúcich otázok, ako aj nutnosť uplatňovať apelačné právo. Dôvodom sú vážne globálne hrozby súvisiace s uvedenou problematikou. Také vážne, že ich niektorí teoretici považujú za vážnejšie ako vojny a konflikty. Možno s výnimkou ľuďmi iniciovanou jadrovou vojnou a globálnou jadrovou katastrofou, ale v konečnom dôsledku aj v tomto prípade sú najviac ohrozené všetky infraštruktúry súvisiace s prežitím ľudstva a ochranou *antickej sebestačnosti* prírody, ktorá bude schopná obnovy.

Prístup k riešeniu problému je v podstate globálna agenda, ktorá nadobudla významný rozmer až v druhej polovici 20. storočia, keď sa agenda súvisiaca so životným prostredím začala meniť z lokálnych/národných hrozieb, cez kontinentálne hrozby, až ku globálnym hrozbám, čím sa do povedomia ľudstva dostali trvalé neistoty, pôsobiace aj v súčasnosti. Táto agenda je teda s novým poznaním napätia medzi národnými cieľmi, cieľmi ekonomických zoskupení/organizácií, ich produkciou, kapitálovými investíciami, ich návratnosťou a výsledným trvalým ohrozovaním životného prostredia, na rôznych úrovniach, ale v podstate v globálnom priestore.

Riešenie problematiky sa odvíjalo počas štyroch období, ktoré odzrkadľujú rôzne úrovne zodpovednosti a poznania vôbec. Súčasťou sú aj rôzne ideológie a koncepty od religióznych až po extrémistické. Priebeh spolupráce štátov na základe uplatňovania vedeckého prístupu k náprave je komunikovaný a koordinovaný prostredníctvom funkčných medzinárodných agentúr, medzinárodných konferencií a globálnych summitov, ktoré nadobudli výraznú účinnosť od prelomu 20. a 21. storočia, aj keď sa v tejto problematike predpokladá dlhodobá príprava i uskutočňovanie záchranného programu pred zmienenou globálnou hrozbou, dnes už s vážnymi bezpečnostnými konotáciami.

Medzi najvýznamnejšie patria:

- Svetová konferencia o životnom prostredí v Štokholme, 1972, kde po prvý krát krajiny uznali svoju zodpovednosť a životné prostredie;
- Svetová komisia pre prostredie a rozvoj, 1983, ktorá v Brundtlandskej správe (1987) definovala nový termín – trvalo udržateľný rozvoj – ako rozvoj, ktorý dokáže naplniť potreby súčasných generácií bez toho, aby bola ohrozená možnosť budúcich generácií napĺňať ich potreby;
- Konferencia OSN v Rio de Janeiro, 1992, ktorá ustanovila, že pre riešenie klimatických zmien je potrebná radikálna zmena správania a zvýšenie environmentálneho povedomia štátov;
- Klimatický summit v Glasgowe, 2021, kde sa štáty o. i. zaviazali prijať opatrenia na znižovanie teploty našej planéty, zvýšiť finančné prostriedky na boj proti klimatickým zmenám pre rozvojové krajiny, zastaviť a zvrátiť stratu lesov a degradáciu pôdy, obmedziť emisie metánu, ktorý je vo vysokej miere zodpovedný za súčasné otepľovanie v dôsledku ľudskej činnosti, ako aj podporiť Juhoafrickú republiku pri prechode od uhlia k nízkouhlíkovému hospodárstvu.

Všetky konferencie a summity mali aj tieto spoločné ciele:

- zákonnosť;
- spravodlivosť;
- vôľa vykonávať činnosť v súvislosti s pravidlami ochrany bezpečnosti na viacerých úrovniach;
- globálnosť – nutnosť zahrnúť do cieľov všetky štáty – udeľovanie výnimiek nie je možné;

- diskusie o stratégiách, ich vykonávaní, teda neoddeliteľnosť od vnútornej a zahraničnej politiky štátov;
- komunikovanie aj s bezpečnostnými stratégiami štátov a bezpečnostných organizácií (NATO, OBSE, a ďalšie);
- komunikácia so subjektami zodpovednými za vývoj nových zbraní a všetkých obranných systémov s tým, že je potrebné uplatňovať konsenzus pri rozhodovaní (Krejčí, 2009, s. 381-382);
- dôraz na energetickú bezpečnosť (Kasinska, 2014, s. 452).

Je predpoklad, že všetky tieto ciele budú zachované aj v najbližšej budúcnosti, pretože bezpečnostná hrozba v súvislosti s environmentálnou problematikou bude mať stále jednu špecifickú črtu – prelínanie problematiky nadnárodnej s nadnárodnou, kontinentálnou a globálnou. Dôkazom toho je aj súčasná situácia extrémneho otepľovania s extrémnym suchom v časti sveta, do ktorej patrí aj Slovenská republika a s extrémnymi záplavami v iných častiach sveta. Tieto vážne disproporcie nie je možné riešiť inak ako medzinárodnou spoluprácou.

2 GLOBALIZÁCIA AKO SPÚŠŤAČ HROZIEB RÔZNEJ IDENTITY

Globalizácia je široko koncipovaný proces, na ktorom sa podieľajú jednotlivé štáty, politické zoskupenia, politicko – ekonomické agregáty typu EÚ, ale aj organizačné pôsobenie medzinárodných a mimovládnych organizácií s rôznou teritoriálnou a politickou pôsobnosťou.

Štáty a organizácie majú možnosť budovať globálne siete, zabezpečujúce chod ekonomiky, fungovanie informačných technológií bez obmedzenia, medzinárodnú politickú a bezpečnostnú spoluprácu, koordináciu inovatívnych funkcií na všetkých úsekoch verejného, ale aj súkromného života. Globálne siete neznamenajú len túto potrebnú komunikáciu, ale aj influencerstvo – teda fabrikovanie vzorov správania, spôsob hovorovej komunikácie, módu (v obliekaní, čítaní, hudbe a kultúre vôbec). Môžu sa stať nositeľmi pokroku, napríklad pri zmene postoja k environmentálnym problémom, k zachovaniu historicky overených pozitívnych spoločenských hodnôt, atď.

Počas tohto procesu dochádza k zaujímavému javu. Najprv začne fungovať globalizácia niečoho vyvolaná spoločenskou potrebou/spotrebou. Potom sa k nim vytvára teória, prečo je to tak. Vzniká nová ideológia mohutného rozsahu, ktorú môžeme nazývať globalizmus. Je to prepájanie všetkého, aj keď svet nie je prepojený fyzicky. Niektoré regióny sa otvárajú svetu, niektoré sa naopak od sveta izolujú. V reálnom čase takéto prepájania produkujú vzory a tie môžu v krajinách, kde ich len prevzali, mať ničivý účinok na spoločnosť. Za všetko spomenieme rôzne závislosti, ktoré s globalizmom narastajú (napr. autoritárstvo, nekontrolovaný liberalizmus, politická pasivita, narastanie extrémistických aktivít a pod.). O závislosti hovoríme z toho dôveru, že najmä v posledných dvoch dekádach zaznamenávame aj v konsolidovaných demokraciách nárast spomínaných aktivít[2].

Ak má byť táto časť explikačná, je potrebné vymedziť si aspoň orientačne terminologický úzus. Aj keď pripustíme, že v globálnom, osudovo prepojenom spoločenstve neexistuje nástojčivo potrebný veľký a akcie schopný subjekt „ľudstvo“, snívame o ňom a chceme aby sa stal skutočnosťou. Ľudstvo by sa malo emancipovať ako vládca nad vlastnými dejinami (ktoré však samo vytvára). Autor týchto kontemplatívnych myšlienok **R. Safranski**

[2]Ako príklad môžeme uviesť nárast extrémistických hnutí dlhodobo budovanej konsolidácii územia Izrael – Palestína, nedoriešený problém statusu Kosova a najmä nedoriešené problémy územnej súčasti bývalého Sovietskeho zväzu ako napr. Podnesterská republika. Všetky tieto zmeny môžu pôsobiť ako potenciálne bezpečnostné hrozby (pozn. autorky).

v knihe *Koľko globalizácie unesie človek?* Podáva zaujímavú interpretáciu pojmu globalizácia – že filozofi pripisujú ľuďom rozum, ktorý je do istej miery a priori založený na konsenze. Preto je možné všetky idey globalizovať. Ale história nás učí, že v duchovných projektoch (čiže v skorších formách globalizmu), aj v súčasných projektoch sa v nich zákonite objavujú konkurenčné návrhy, alebo odsudzujúce, úplne zamietavé koncepty, ktoré ideu globálneho dobra pre ľudstvo neakceptujú. Odmietanie môže nastať ihneď, ako začne idea globalizácie fungovať, alebo nastane postupom času, keď je „globálne dobro" pociťované ako obmedzovanie, zavádzanie, dokonca ako bezpečnostná globálna hrozba.

Typickým príkladom je náboženstvo. Vznik náboženských systémov od najstarších čias, cez kresťanstvo až po súčasné fundamentalistické náboženské hnutia už pri svojom vzniku vyvolával a vyvoláva odpor inak orientovaných jedincov, ale aj spoločenských skupín a oficiálnych štátnych štruktúr. Dôvodom je vždy obava o stratu vlastného postavenia, moci i vlády, najmä vtedy, ak náboženské idey obsahujú presvedčivú argumentáciu pre zlepšenie života. Zlepšenie môže spoločnosť vyžadovať aj v materiálnej, ale aj duchovnej sfére. Hlavnou témou prijatia ideí vo všetkých náboženstvách je totiž oslobodenie človeka od rôznych foriem útlaku, ponižovania a najmä oslobodenie mysle, rozumu a srdca. Veriaci človek sa vyrovnáva s problémami oveľa statočnejšie ako ten, čo neverí v dobro. Tieto premeny však vyvolávali strach najmä vo vládnucej triede, ktorý postupne prerastal do prenasledovania veriacich v dobro – čo je eufemizmus napr. pre kresťanskú vieru – ale stal sa i príčinou náboženských vojen typických pre ranný stredovek, aj keď myšlienka prenasledovania „pohanov" ako trest za inú religiozitu sa postupne transformovala na dobyvateľské vojny medzi štátmi za účelom získania územia, ktoré mohlo dobyvateľom poskytnúť mnohé benefity (Carroll, 1996).

Rôzne teoretické prístupy k tejto téme sú v novovekej histórii predmetom skúmania v mnohých vedných disciplínach od historiografie, politických vied, dejín náboženstva, ale aj geografie, kulturológie a tiež bezpečnostnej vedy.

Dôvodom sú vyššie spomenuté ambície súperiacich spoločenských komunít – tých komunít, ktoré neprijímajú náboženské (väčšinou striktné) predpisy ako spôsob existencie ľudí, komunít, národov, štátov, s tými komunitami, ktoré v náboženstve a v dodržiavaní religióznych princípov vidia iný, lepší spôsob existencie jednotlivcov, ale aj rodín a všetkých hierarchických stupňov spoločnosti.

V tomto súperení existujú rôzne spôsoby komunikácie. Presviedčanie, agitácia prostredníctvom príkladov, dôraz a kontrola dodržiavania religióznych princípov, ale aj nenávisť, tresty, hrozby až po potieranie všetkých humánnych komunikačných prostriedkov, ktoré sú základným znakom konfliktov a vojen.

Problémom je, že na rozdiel od väčšiny vojen v predchádzajúcich storočiach, ktoré mali špecifický charakter – koloniálnych, dobyvačných a strategicko – politických, súvisiacich s rozpadom ríše, ale aj naopak so zjednocovaním územia do jedného celku – aby sme spomenuli aspoň niektoré, súčasné vojny možno označiť ako dobyvačné tiež, ale dôvody sú politické – zmena režimu, spôsobu vlády a tým aj komunikácie v medzinárodných vzťahoch s tým, že štát, ktorý bol definovaný ako príčina zásahu/agresie zo strany iného štátu už nebude môcť v budúcnosti vystupovať ako trvalá hrozba nielen pre susedné štáty, ale aj v globálnom zmysle.

K politickým dôvodom ako motivácii pre ozbrojený konflikt sa pridružujú iné faktory, najmä také, ktoré v minulosti neboli a dokonca ani nemohli byť súčasťou vojny (Marshall, 2015), najmä vďaka mnohým mierovým zmluvám v Európe, ale aj na iných kontinentoch, ktorých podstatou bolo, že vychádzali z Aristotelových požiadaviek na tzv. spravodlivú vojnu (napr. Vestfálsky mier, Versaillská zmluva, a iné).

Novým fenoménom na prelome 20. a 21. storočia je tzv. hybridná vojna (Zaplatynski, 2015). Ako uvádza autor, vojenský konflikt na Ukrajine, ktorý je predmetom analýzy v

citovanej štúdii pravdepodobne ovplyvní osud celej Európy (tamže, s. 375). Konflikt nazývaný hybridnou vojnou vždy začína dávno predtým, ako nadobudol charakter vojny. Hybridnej preto, lebo okrem územno - politických príčin sa tu preukázateľne problémy transformovali do ekonomických (plyn, jeho výskyt, tranzit, ďalšie ekonomické konotácie s tým súvisiace), ďalej tu bola otázka národnostná (historický relikt), otázka týkajúca sa poľnohospodárstva a tiež využívania teplovodných prístavov, aby sme spomenuli aspoň tie najdôležitejšie. Konflikt, ktorý teda začal v polovici dekády medzi rokmi 2010 – 2020 a v súčasnosti sa zmenil na vojenskú agresiu jedného štátu voči svojmu susedovi, stále trvá. A neovplyvnil len osud celej Európy (EÚ ale i nečlenské štáty), ale aj globálnu bezpečnosť. Stal sa globálnou hrozbou a je možné, že aj ďalšou fázou Studenej vojny, pretože sa do jeho riešenia zapojili aj USA s tým, že je v plnej miere rešpektovaný čl. 5 Severoatlantickej zmluvy.

Je len otázkou času, či bude v budúcnosti na Ukrajine dlhodobo potrebné a možné uskutočňovať mierové operácie OSN, čo už samo o sebe evokuje víziu globálnej hrozby, ktorá sa ukazuje na území strednej a východnej Európy aj v štátoch, ktoré sú členmi NATO (Jurčák, Ivančík, 2015).

Ďalšie nebezpečenstvo z možného konfliktu, ktoré sa môže týkať aj štátov zatiaľ imúnnych voči náboženským konfliktom, ako sme uviedli na začiatku tejto časti, je obava z *kvázi* hybridnej vojny, alebo presnejšie hybridného konfliktu, ktorý by sa týkal prenikania extrémistických a fundamentalistických ideí šírených zo strany migrantov.

Súčasný príliv migrantov do Európy je spôsobený viacerými faktormi. Migrácia je pojem, ktorý však nevystihuje podstatu problému. Pre javy súvisiace so súčasnou migráciou sa používa termín vysťahovalectvo, osoby súvisiace s týmto termínom sa delia na dobrovoľných emigrantov, nútených migrantov a utečencov. Trasy a ciele si utečenci vyberajú na základe poznatkov o krajinách, kde možno existuje systém, ktorý ich umožňuje prijať a domestikovať. V 19. storočí to boli najmä USA a Argentína na americkom kontinente, v 20. storočí tiež a okrem toho európske ekonomicky silné štáty ako Veľká Británia, Francúzsko, Nemecko a Belgicko. Najväčšie vlny prisťahovalcov do týchto štátov odchádzali pred a po I. a II. svetovej vojne, počas veľkej hospodárskej krízy v 30. rokoch 20. storočia a počas tzv. totalitného režimu, do ktorého patrili okrem územia ZSSR aj štáty strednej Európy a Balkánu.

Prispôsobovanie sa novým pomerom záviselo od prijímajúceho štátu, nakoľko bol tolerantný k inej kultúrnej a náboženskej identite cudzincov, ako sa dokázali prispôsobiť režimu a sociálnemu úzusu. V podstate sa problémy s migráciou, ktorá sa v mnohých médiách prezentuje často ako bezpečnostná hrozba, začali v dekádach 2000 – 2020 (Matlary, 2007). Spočiatku sa zdalo, že domáca i prijatá komunita spolu komunikujú na adekvátnej úrovni. Pravdepodobne až prudký nárast počtu migrantov po roku 2015 spôsobil medzi Európanmi doslova fóbiu z budúcnosti. Nedostatočné možnosti poskytovania azylových domovov, nedostatočný počet dokladov totožnosti sprísnili kritériá poskytovania azylu a ďalšie koncepty domestikácie. Zo strany migrantov začalo dochádzať v oveľa väčšom množstve ako v predchádzajúcich rokoch k prejavom nespokojnosti, ktoré sa často kvalifikovali ako násilie, terorizmus, extrémizmus i fundamentalizmus. V skutočnosti sa naozaj udiali takto prezentované udalosti, ale boli zriedkavé a zveličované, až prerastali do rasizmu a extrémizmu zo strany domáceho obyvateľstva voči prisťahovalcom. Tento trend je označovaný ako trvalý a existujú obavy, že aj v štátoch EÚ bude dochádzať k násilným činom ako v USA a tiež vo Veľkej Británii.

Aj pri udelení statusu občana emigrantovi v prijímajúcom štáte je dôležité, či tento štát dokáže zabezpečiť verejný poriadok, ochranu domácich občanov ako prioritu a tiež ochranu domácej a európskej identity. To isté platí aj na americkom kontinente – v USA, Kanade, tiež na Blízkom a Strednom Východe, kde dochádza k miešaniu občanov s rôznymi typmi islamu (Šrobár, 2015).

Problémom je, že domáci občania vedome alebo nevedome podstupujú sekularizáciu. Vedome – ak sa dobrovoľne vzdávajú náboženskej viery a pravidiel, ktorými sa viera prezentuje v duševnom i spoločenskom živote. Nevedome vtedy, ak už s výmenou generácií dochádza aj k pozvoľnému zániku pravidiel náboženskej viery z dôvodu prijatia iného hodnotového systému.

Sekularizácia (vedomá ani nevedomá) neovplyvňuje život prisťahovalcov, príslušníkov svojho bývalého domova, kde žili napr. podľa zákonov islamu. Vedome a programovo popierajú striktné oddelenie náboženskej viery od všetkých ostatných sfér, najmä od politickej, spoločenskej a kultúrnej. Akákoľvek činnosť silných, nábožensky založených moslimov má byť podľa nich vykonávaná podľa náboženských meradiel. Týka sa to jednotlivca, rodiny, aj komunity. Zahŕňa aj odmietanie sociálneho poriadku, aký vyžaduje prijímajúci štát, ak je v rozpore s vyššie uvedeným pravidlom. Spočiatku vnútorný problém štátov, alebo presnejšie vnútorná bezpečnostná hrozba, v súčasnosti prerastá do globálnej hrozby konfliktov na území štátov, kde žijú migranti so silným sklonom opozície voči domácim pravidlám. Postupne však narastá globálne rozširovanie fundamentalizmu islamského, v menšom meradle židovského, kresťanského prejavujúceho sa najmä vo variabilných systémoch viery, v rôznych sektách a zoskupeniach.

Výskyt fundamentalizmu a jeho rozširovanie znamená, že sekularizácia nebola dokončená do tej miery, aby nábožensky cítiaci prisťahovalci neboli terčom posmechu, odmietania, ale aj násilných činov. Viac to však platí opačne. Posmech, odmietanie a násilné činy sú realizované na domácom obyvateľstve, pretože sa urážlivo správa voči inej viere.

Ak by sme mali znova spomenúť **Machiavelliho**, aj tu ide o moc, ale nie politickú. Ide o moc náboženstva nad inými zložkami sociálnej sféry, nielen o akceptáciu. V hre je vlastne boj o moc v politike, ktorá musí byť podriadená náboženstvu.

V podstate ide o čas. Ak sa sekulárne štáty nestanú imúnne voči prejavom fundamentalizmu, môže to znamenať novú globálnu hrozbu, ktorá bude prechádzať po generačnej línii.

Štáty, ktoré sú, alebo budú takto ohrozené, väčšinou na hrozbu reagujú racionalistickým kódexom. Práve s ním súvisí aj celkové prehodnotenie histórie, najmä čo sa týka hodnoty náboženstva a jeho spoločného prínosu pre spoločnosť. Jedným z takýchto snáh bol aj etablovaný koncept marxistickej filozofie, ktorá náboženstvo označovala za ópium ľudstva. Projekt odstrániť náboženstvo a tým aj zárodky fundamentalizmu v spoločnosti v marxisticky orientovaných krajinách neuspel, naopak posilnili sa práve fundamentalistické črty kresťanstva. Problém je asi v tom, že sekulárne kritériá nemôžu byť jedinými kritériami, ktoré pomôžu rozvoju štátu v globálnej spoločnosti (Hovellebeck, 2002).

ZÁVER

Z hľadiska globálnej bezpečnosti je možná klasifikáciu hrozieb podľa objektívnej pôsobnosti vnímať ako alternatívu výskumu, ale nesmie sa stať jedinou a trvale platnou. To je vo vede možné len v zriedkavých prípadoch. Preto sme v texte uviedli aj originálnu a v podstate modernú myšlienku starogréckeho filozofa **Parmenida** o neoddeliteľnej súvislosti vzniku sveta a jeho trvalej sebestačnosti, t. j. schopnosti zachovať si svoj pôvodný prírodný stav.

Otázkou, ktorá bola riešená aj v predloženej štúdii je, či je ľudstvo v súčasnosti schopné tento pôvodný stav ochrániť. Napríklad tým, že terajšie hrozby budú zmiernené, alebo odstránené plodnou spoluprácou aj v oblasti bezpečnostnej politiky.

V tejto téme existujú dva rozdielne názory: 1) globálna bezpečnosť musí byť kooperatívna, inak nemá nádej na úspech; 2) globálna bezpečnosť nepotrebuje kooperáciu, len koordináciu v zahraničnej politike. Autorka sa prikláňa k prvému názoru, jej snahou bolo

použiť pre to racionálne argumenty, ktoré vypracovali generácie pôsobiace vo vede a výskume bezpečnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BREGMAN, R. 2020. *Ľudskosť. Optimistická história človeka*. N Press s. r. o.. 2020. 464 s. ISBN 978-80-99925-38-1.

CARROL, J. 1996. *Humanizmus. Zánik západní kultury.* Brno: Centrum pro studium demokracie a kultury. 1996. 199 s. ISBN 80-85959-13-5.

CYGANKOV, P. A. 2003. *Teorija meždunarodnych otnošenij.* Moskva: Gardariki. 2003. 587 s. ISBN 5-8297-0106-5.

GOENTSHOM, G., BERNAYS, E. 1986. The Origins of Threats. In: KEEN, S. *Faces of the Enemy. Reflection of the Hostile Imagination: The Psychology of Enmity.* New York: Harper and Row. 1986. 200 s. ISBN 9780062504722.

JAUROVÁ, Z. 2013. Sen o ozajstnej krajine. In: *Odkiaľ a kam. Zborník 20 rokov samostatnosti.* Bratislava: Inštitút pre verejné otázky a Kalligram. S 409 - 420. ISBN 978-80-89345-42-7.

JURČÁK, V., IVANČÍK, R. 2015. Základné princípy uskutočňovania mierových operácií OSN. In: *Bezpečnostné fórum 2015 – Zborník vedeckých prác, II. zväzok. Banská Bystrica: Belianum.* 2015. S. 535-542. ISBN 978-80-557-0850-8.

KASINSKA, M. 2014. World economic security in the years 2000 – 2015. In: *Bezpečnostné fórum 2014 – Zborník vedeckých prác, II. zväzok.* Banská Bystrica: Belianum. 2014. S. 444-455. ISBN 978-80-557-0678-8.

KOLAKOWSKI, L. 1999. *Metafyzický horor.* Mladá fronta. 1999. 136 s. ISBN 80-204-0767-7.

KORZENIOWSKI, L. F. 2008. *Sekuritologia.* Krakow: EAS. 2008. 312 s. ISBN 978-83-925072-1-5.

LASICOVÁ, J., UŠIAK, J. 2013. *Bezpečnosť ako kategória.* Bratislava: Veda. 2013. 264 s. ISBN 978-80-224-1284-1.

MARENČINOVÁ, V. 2019. Informačno – komunikačné technológie ako nástroj rodovo podmieneného násilia. In: Interpolis ´18 – Zborník vedeckých prác. Banská Bystrica: Belianum. 2019. S. 181-188. ISBN 978-80-557-1536-0.

MARSHALL, T. 2017. *V zajatí geografie.* Bratislava: Premedia. 2017. 248 s. ISBN 978-80-8159-513-4.

MATLARY, J. H. 2007. *Ľudské práva ohrozené mocou a relativizmom.* Prešov: Vydavateľstvo M. Vaška. 2007. 221 s. ISBN 97-880-7165-648-7.

SAFRANSKI, R. 2006. *Koľko globalizácie unesie človek?* Bratislava: Kalligram. 2006. 96 s. ISBN 80-7149-858-8.

ŠROBÁR, Š. 2015. Motívy náboženského terorizmu. In: *Medzinárodná vedecká konferencia Bezpečnosť, extrémizmus, terorizmus 2015. Zborník prednášok.* Podhájska: Agentúra Rozvoj. 2015. s. 149-153. ISBN 978-80-89608-29-4.

ZAPLATYNSKYI, V. 2015. Bezpečnosť v Európe a hybridná vojna na Ukrajine. In: *Bezpečnostné fórum 2015 – Zborník vedeckých prác, II. zväzok.* Banská Bystrica: Belianum. 2015. S. 375-385. ISBN 978-80-557-0850-8.

PhDr. Veronika GAŠKOVÁ
Externá doktorandka
Akadémia ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši, Demänová 393, Liptovský Mikuláš 031 01.
weron0605@gmail.com

CIELE A PLÁNOVANÉ DOPADY SANKCIÍ PROTI RUSKU OD ZAČIATKU INVÁZIE NA UKRAJINU

TARGETS AND PLANNED IMPACTS OF SANCTIONS AGAINST RUSSIA FROM THE BEGINNING OF THE INVASION TO UKRAINE

Marek HARGAŠ

ABSTRACT

As the Russian invasion of Ukraine enters into its eight month, a common narrative has emerged that the unity of the world in standing up to Russia has somehow devolved into a war of economic attrition which is taking its toll on the west, given the supposed "resilience" and even "prosperity" of the Russian economy. In this article we are trying to show how these statements are simply untrue. From our analysis, it becomes clear: business retreats and sanctions are crippling the Russian economy, in the short-term, and the long-term. We tackle a wide range of common misperceptions – and shed light on what is actually going on inside Russia

Keywords: Sanctions, Russia, Ukraine, Oil and Gas Export.

ÚVOD

Ciele medzinárodných sankcií uvalených voči Rusku sú jasné. Oslabiť „protivníka" ekonomicky, ochromiť jeho výrobné kapacity, obmedziť pohyb a výhody politických elít a oligarchov, čím by sa mal vyvinúť tlak ako na každodenného občana, tak aj na vedenie krajiny a jeho rozhodovanie. Menej jasné je, ako dlho to môže trvať a čo všetko to bude stáť krajiny zavádzajúce sankcie. V tejto práci sme sa snažili zamerať na aktuálny stav Ruskej federácie v kľúčových oblastiach a prognózy do budúcna, o ktorých kvôli nedostatku hodnoverných informácií a dát panujú rôzne dezinformácie.

Ruská invázia na Ukrajinu viedla takpovediac k otvoreniu priehrady so sankciami. Malý pramienok už existujúcich sankcií, ktoré Európska únia, USA a ďalšie štáty uvalili na Rusko po anexii Krymu, sa zmenila na cunami vážnych ekonomických opatrení. Nových balíčkov sankcií v priebehu času a počas celej dĺžky konfliktu stále pribúda, zatiaľ môžeme doteraz uvalené sankcie rozdeliť do šiestich kategórií.

Prvá kategória opatrení sa týka ruského politického a ekonomického vedenia, elít, a má podobu kompletného zmrazenia majetku. Tieto sankcie sa dotkli hlavne prezidenta Putina a ďalších členov ruského parlamentu, avšak v marci 2022 Spojené štáty americké oznámili, že zvažujú uvalenie sekundárnych sankcií, ktoré by zakazovali zahraničným firmám, ktoré obchodujú so sankcionovanými ruskými subjektmi, prístup na americký trh (Stein, Whalen, 2022).

Druhá kategória opatrení je zameraná na ruský finančný systém, čo zahŕňa zablokovanie hlavných ruských bánk a finančných inštitúcií od systému SWIFT. Dôležitým krokom zo strany EÚ a USA bol zákaz všetkých transakcií s Centrálnou bankou Ruskej federácie. Toto opatrenie má za úlohu zabrániť Rusku oslabiť dopad sankcií tým, že získa prístup k svojim obrovským devízovým rezervám.

Tretia kategória je venovaná energiám. Spojené štáty zakázali dovoz ruskej ropy, LNG (skvapalnený zemný plyn) a uhlia, ako aj akékoľvek investície do ruského energetického

sektoru. Po prvotnom zdráhaní sa musela aj EÚ začiatkom apríla 2022 pristúpiť k tomuto kroku, ktorý určitým spôsobom ohrozuje energetickú bezpečnosť celej únie, nielen krajín, ktoré vo veľkom závisia od ruských dodávok plynu.

Štvrtá kategória sankcií je zameraná na iné kontrolné mechanizmy medzinárodného obchodu, s účelom zmariť prístup Ruska k nevyhnutným komoditám a technológiám, čo by podľa plánu malo viesť k oslabeniu jeho vojenských akcií. V marci 2022 EÚ, USA, Kanada a ďalšie štáty G7 sa zaviazali zrušiť Rusku status doložky najvyšších výhod (eng. most-favored-nation), čo efektívne maže všetky benefity členstva v Svetovej obchodníckej organizácii (WTO). Tieto opatrenia boli spojené s viacerými reštrikciami týkajúcimi sa investícií, ako aj s rozhodnutím Nemecka neudeliť certifikát plynovodu Nord Stream 2 (Marsh, Chambers, 2022).

Piatou kategóriou je transport. Okrem iného majú ruské aerolínie zakázané vstup do vzdušného priestoru množstva krajín vo svete a EÚ spolu s USA požadovali od lízingových firiem, aby skonfiškovali všetky lietadlá zapožičané ruským aerolíniám. Ruská vláda si na druhej strane ako odvetu zabavila komerčné lietadlá vo vlastníctve západných lízingových spoločností (Isidore, Liakos, 2022)

Posledná kategória sankčných opatrení súvisela s odchodom privátneho sektoru z Ruska. Množstvo zahraničných firiem opustilo ruský trh, čomu sa budeme bližšie venovať neskôr.

V nasledujúcej kapitole stručne zhrnieme niektoré sankcie a najdôležitejšie dátumy a v tej ďalšej sa budeme venovať konkrétnym oblastiam, ktoré podľa nášho názoru najvernejšie odzrkadľujú skutočný stav ruskej ekonomiky a predpokladaný vývoj do budúcna a tým aj schopnosť dlhodobo viesť vojenské operácie.

1 STRUČNÝ PREHĽAD VÝZNAMNÝCH SANKCIÍ PO ZAČIATKU INVÁZIE

Už pred začiatkom ruských vojenských akcií na Ukrajine 24. februára 2022 boli v platnosti reštriktívne opatrenia EÚ súvisiace s nezávislosťou a teritoriálnou integritou Ukrajiny, týkajúce sa 193 jednotlivcov a 48 subjektov. Jednotlivcom bol zmrazený majetok a dostali zákaz cestovania na území EÚ (medzi nimi napríklad traja členovia ruského parlamentu, ktorí boli zvolení vo voľbách v septembri 2021 ako reprezentanti Krymu a mesta Sevastopoľ).

Spolu so svojimi spojencami odsúhlasili 22. februára ministri zahraničných vecí členských krajín EÚ rozšírenie sankcií so zameraním na:

- 351 členov ruského parlamentu, ktorí hlasovali za uznanie Doneckej a Luhanskej ľudovej republiky,
- 26 jednotlivcov a subjektov, ktoré hrali úlohu v podrývaní a ohrozovaní teritoriálnej integrity Ukrajiny, jej nezávislosti a samostatnosti, a to vrátane bánk, ktoré financujú rôzne rozhodovacie orgány, ďalej sektor obrany, ktorý hral úlohu v invázii a je zodpovedný za vedenie dezinformačnej vojny proti Ukrajine (na zozname je napr. minister obrany Ruskej federácie Sergej Šojgu),
- Obchodné aktivity Doneckej a Luhanskej ľudovej republiky do a z EÚ,
- Prevenciu pred prístupom Ruska a vládnych orgánov k európskemu kapitálu a finančným trhom a službám.

Vysoký predstaviteľ únie pre zahraničné veci a bezpečnostnú politiku Josep Borell potvrdil, že EÚ bude „výrazne zvyšovať úroveň sankcií podľa správania sa Ruska“(EU External Action Service, 2022).

Na doplnenie týchto balíčkov sankcií prijala EÚ koncom júla opatrenia, ktoré majú za úlohu lepšie prepojiť a viac zefektívniť už existujúce sankcie.

Podľa Európskej komisie sú tieto sankcie určené na:

- Ochromenie schopnosti Kremľa financovať vojenské akcie.
- Uvaliť jasné ekonomické a politické náklady na ruské politické elity, zodpovedné za inváziu.
- Znížiť ruskú ekonomickú základňu (European Commission, 2022).

Na sankčný zoznam boli pridaní prezident Putin aj ruský minister zahraničných vecí Sergej Lavrov, ďalej členovia ruskej národnej bezpečnostnej rady a členovia ruského parlamentu, ktorí zatiaľ neboli na zozname. Únia ďalej zmenila kritéria zaradenia na sankčný zoznam tak, aby sa dal rozšíriť o jednotlivcov a firmy, ktoré podporujú a profitujú z úzkych vzťahov s ruskou vládou, ako aj na rodinných príslušníkov týchto jednotlivcov. Rovnako odsúhlasili lídri EÚ aj zavedenie sankcií voči Bielorusku, pre jeho úlohu v ruskej agresii na Ukrajine.

Začiatkom marca boli predložené návrhy na zabezpečenie a zjednodušenie účinnej konfiškácie majetku jednotlivcov a subjektov, ktoré porušujú reštriktívne opatrenia. Návrhy sa predkladali v kontexte pracovnej skupiny na zaisťovanie a konfiškáciu majetku s názvom „Freeze and Seize Task Force“, ktorá bola v rovnaký mesiac na tieto účely zriadená. Európska komisia navrhla, aby sa porušenie reštriktívnych opatrení zaradilo do zoznamu trestných činov EÚ, čo umožní stanoviť spoločný základný trestnoprávny štandard a sankcie v celej únii. Takéto spoločné pravidlá EÚ môžu uľahčiť vyšetrovanie, stíhanie a trestanie porušení reštriktívnych opatrení vo všetkých členských štátoch. Dôležitou skutočnosťou je, že nová pracovná skupina bude spolupracovať s už existujúcou skupinou REPO (Ruské elity, zástupcovia a oligarchovia, angl. Russian Elites, Proxies and Origarchs), vytvorenou Spojenými štátmi, EÚ, Spojeným kráľovstvom a ďalšími spojencami.

Komisár pre spravodlivosť a spotrebiteľov Didier Reynders v tejto súvislosti uviedol: *„Musíme zabezpečiť, aby osoby alebo spoločnosti, ktoré obchádzajú reštriktívne opatrenia EÚ, za to niesli zodpovednosť. Takéto konanie je trestným činom, ktorý by sa mal prísne postihovať v celej EÚ. V súčasnosti môžu rozdielne trestnoprávne definície a sankcie, pokiaľ ide o porušenie reštriktívnych opatrení, stále viesť k beztrestnosti. Musíme odstrániť medzery a poskytnúť justičným orgánom vhodné nástroje na stíhanie porušení reštriktívnych opatrení Únie“ (Európska komisia, 2022).*

1.1 BANKY A FINANČNÉ TRHY

Rozšírené boli aj už existujúce sankcie obmedzujúce prístup Ruska na finančné trhy únie. Ruské banky, vrátane Ruskej centrálnej banky, majú zákaz akejkoľvek formy požičiavania či nakupovania cenných papierov. Plnohodnotné zmrazenie aktív bolo uvalené na tri hlavné ruské banky a zoznam štátom vlastnených podnikov, na ktoré sa budú vzťahovať sankcie bol rozšírený o sektor obrany. Ruskí jednotlivci majú zákaz ukladania peňazí do bánk v EÚ nad určitú hodnotu.

V ďalšom rozšírení sankcií, oznámenom 2. marca, pridala EÚ na zoznam postihnutých aj Ruský fond priamych investícií a vyhlásila, že predaj, dodanie, transfer alebo export denominovaných euro bankoviek bude zakázaný (Official Journal of the European Union, 2022). Tento zákaz bol 8. apríla 2022 ďalej rozšírený bankovky v akejkoľvek oficiálnej mene členských štátov EÚ (Council of the European Union, 2022).

Dňa 9. marca EÚ potvrdila, že finančné reštrikcie sa budú týkať aj krypto majetku, „čím sa zabezpečí patričná implementácia sektorových reštrikcií“ (Council of the EU, 2022a). Ďalej 8. apríla EÚ oznámila úplné zmrazenie majetku štyroch ruských bánk: Okritie, VTB, Sovcombank a Novikombank, (Official Journal of the European Union, 2022b) ako aj všeobecný zákaz participácie ruských firiem vo verejných obstarávaniach v členských štátoch

únie a vylúčenie všetkej finančnej podpory pre ruské verejné inštitúcie (Council of the EU, 2022b).

Ako súčasť šiesteho balíčka sankcií boli 3. júna potvrdené ďalšie tri banky: Sberbank, Credit Bank of Moscow a Ruská poľnohospodárska banka, ktoré mali byť odstrihnuté od medzinárodného platobného systému SWIFT.

1.2 SEKTOROVO ŠPECIFICKÉ OBCHODNÉ REŠTRIKCIE

EÚ zaviedla zákaz exportu špecifických tovarov a technológií súvisiacich so sektorom rafinácie ropy, leteckým a vesmírnym priemyslom a tovarov a technológií dvojakého použitia súvisiacich s obranným priemyslom, vrátane polovodičov a technológií ako sú drony a príslušný softvér. Reštrikcie platia aj na súvisiace služby. Dňa 9. marca EÚ pridala zákaz exportu systémov námornej navigácie a rádiokomunikačné technológie do Ruska (Council of the EU, 2022a) a neskôr (15. marca) únia oznámila, že zakáže všetky transakcie s konkrétnymi štátom vlastnenými podnikmi, ako aj nové investície do ruského energetického sektoru a zákaz vývozu tovaru, technológií a služieb súvisiacich s energetickým priemyslom. V spolupráci so spojencami boli oznámené aj ďalšie sankcie na železo, oceľ a luxusný tovar (Official Journal of the European Union, 2022a).

Lídri EÚ odsúhlasili 8. apríla zákaz na nákup, import alebo transfer uhlia a iných pevných fosílnych palív do EÚ, ak pochádzajú z Ruska alebo sú exportované z Ruska. Tento zákaz začal platiť od augusta 2022. Ďalšie zákazy z apríla sa týkali exportu leteckého paliva, kvantových počítačov a iných pokročilých polovodičov, vysokej elektrotechniky, softvéru, či senzitívnych mechanizmov. Zakázaný bol aj dovoz z Ruska, a to konkrétne dreva, cementu, hnojív, morských plodov a alkoholických výrobkov a sankcie boli ďalej rozšírené na podniky, ktorých výrobky alebo technológie hrali nejakú úlohu v invázii na Ukrajinu, vrátane lodeníc Jantar a PO More Shipyard.

EÚ ďalej odsúhlasila 3. júna 2022 postupný zákaz na nákup, import alebo transfer ruskej surovej ropy a určitých ropných výrobkov v časovom horizonte 6 až 8 mesiacov. Na dovoz surovej ropy cez ropovod však budú existovať dočasné výnimky pre niektoré krajiny, vrátane Slovenska, ktoré je takmer úplne závislé od dodávok cez ropovod Družba.

V súlade s reštrikciami, ktoré už boli zavedené v USA aj Spojenom kráľovstve, potvrdila EÚ zákaz poskytovania účtovných, public relations, konzultačných aj cloudových služieb pre Rusko.

Bezvízový styk pre ruských diplomatov, oficiálnych predstaviteľov a obchodníkov bol pozastavený. Ministri zahraničných vecí 9. septembra 2022 vyzvali na sprísnenie a zdraženie vydávania víz medzi EÚ a Ruskom, čím by všetci ruskí občania museli čakať na udelenie víz 15 dní namiesto 10 a cena by stúpla na 80€ z doterajších 35€.

Predsedníčka Európskej komisie 27. februára oznámila, že všetky ruské lietadlá budú podliehať zákazu vstupu do vzdušného priestoru štátov EÚ. V súvislosti so zákazmi vydanými úradmi v Spojenom kráľovstve, bol 8. apríla oznámený zákaz používania prístavov EÚ plavidlami registrovanými pod ruskou vlajkou. Výnimky budú tvoriť plavidlá s poľnohospodárskym a potravinárskym tovarom na palube, či humanitárna pomoc a energetické výrobky. Ďalej únia oznámila zákaz cestnej dopravy z Ruska a Bieloruska, čím sa má zabrániť rozvozu ruských výrobkov po cestách v rámci EÚ. Aj v tomto prípade existujú výnimky ako humanitárna pomoc, či farmaceutické a medicínske produkty.

S efektívnosťou od 2. marca 2022 boli v EÚ zakázané viaceré štátom vlastnené médiá, vrátane RT a Sputnik. Ďalšie štátom vlastnené médiá boli pridané na zoznam zakázaných 3. júna z dôvodu ich manipulácie s informáciami a propagovania dezinformácií o invázii na Ukrajine s cieľom destabilizovať krajiny susediace s Ruskom, EÚ a jej členské štáty. Jednalo sa o stanice Rossiya RTR, Rossiya 24 a TV Centre International (Council of the EU, 2022c).

1.3 SANKCIE PROTI JEDNOTLIVCOM

28. februára bolo pridaných ďalších 26 jednotlivcov a jeden subjekt na sankčný zoznam EÚ pôsobiacich v ropnom, bankovom a finančnom sektore, vo vláde a ruskej armáde. Medzi jednotlivcami boli napríklad Igor Sečin, riaditeľ Rosneft-u, Nikolaj Tokarev, riaditeľ Transneftu, či Dmitrij Peskov, hovorca prezidenta Putina. Začiatkom marca bolo potvrdené pridanie 160 jednotlivcov na zoznam EÚ, medzi nimi 14 ruských oligarchov a 146 členov Rady Ruskej federácie, ktorí ratifikovali zmluvy o priateľstve, spolupráci a vzájomnej pomoci medzi Ruskom a Doneskou a Luhanskou ľudovou republikou vo februári 2022. Ďalších 15 jednotlivcov bolo pridaných na zoznam 15. marca, vrátane Romana Abrahamoviča, ktorý už bol sankcionovaný zo strany Spojeného kráľovstva. Dôležitým dátumom bol 21. apríl, kedy bol na zoznam sankciami postihnutých osôb pridaný Jevgenij Prigožin, zakladateľ a neoficiálny líder skupiny tzv. Vagnerovcov. V priebehu júna boli sankcie rozšírené na ďalšie osoby spájané s propagáciou a schvaľovaním ruskej invázie na Ukrajinu, vojenskí lídri zodpovední za zločiny spáchané ruskými vojskami v Buči a Mariupole, ako aj rodinní príslušníci už sankcionovaných oligarchov. Na zoznam osôb bol ďalej 4. augusta pridaný bývalý ukrajinský prezident Viktor Janukovyč aj jeho syn Olexsandr, za ich úlohu v podkopávaní ukrajinskej teritoriálnej integrity a stability. Olexsandr Janukovyč je obvinený aj zo spolupráce so separatistickými skupinami na Donbase (Council of the EU, 2022d).

2 DETAILNEJŠÍ POHĽAD NA KONDÍCIU RUSKA V SÚVISLOSTI SO ZEMNÝM PLYNOM A ROPOU

2.1 ZEMNÝ PLYN

Jednou z kľúčových komodít, pri ktorej je – na rozdiel od dezinformačného naratívu – Rusko oveľa viac závislé na Európe, ako Európa od Ruska, je zemný plyn. Zároveň však odzrkadľuje zložité vzťahy medzi krajinami, kedy sa obmedzenie jeho dodávok z Ruska niektorých dotkne podstatne viac, ako iných.

Kľúčovým faktorom na zníženie zraniteľnosti Ruska v jeho asymetrickom vzťahu vzájomnej závislosti s Európou – a zároveň znižujúcim závislosť Ruska od starších plynovodov na území Ukrajiny – bola stavba Nord Stream 1 (prvá linka v roku 2011, druhá 2012) s celkovou kapacitou 55 bcm (bcm = miliarda kubických metrov), ktorá umožnila Rusku priamo zásobovať Nemecko a iné západoeurópske krajiny plynom privádzaným potrubím, obchádzajúc celú Ukrajinu. Stavba Nord Stream 2, ktorá by pridala ďalších 55 bcm kapacity (v prípade, že by bola otvorená, čo dnes už vieme, že nebude) v kombinácii s ďalšími trasami transportu plynu, ako napr. Turkstream (31,5 bcm), by umožnila Rusku aj naďalej obchádzať ukrajinský tranzitný plynový systém (GTS – Gas Transport System), ktorý predstavoval exportnú trasu do Európskej únie. Maximálna ročná kapacita ukrajinského GTS je 146 bcm, približne rovnaká, ako všetkých ostatných exportných trás z Ruska do krajín EÚ dokopy. Gazpromom navýšený tranzit plynu cez Nord Stream 1 v priebehu posledného desaťročia predstavoval významnú platformu, skrz ktorú mohlo Rusko uskutočňovať svoju politiku.

Pochopiteľne, nie všetky európske krajiny boli úplne nevidomé a neuvedomovali si nebezpečenstvá súvisiace s navyšovaním importu ruského plynu cez Nord Stream 1. Napriek tomu, že pôvodne bol ruský plyn zamýšľaný iba ako dočasná alternatíva, kým sa nedosiahne energeticky nezávislejšia budúcnosť, v krátkodobom horizonte používali mnohí experti tento argument za akési ospravedlnenie nečinnosti alebo nedostatku politickej vôle. Napríklad Nemecko si založilo celú svoju ideu o obnoviteľných zdrojoch energie, ku ktorým by sa malo dostať pomocou preklenovacieho paliva – ruského plynu – na základe tejto dočasnosti. Nemecký energetický prechod bol postavený na predpoklade lacného ruského zemného plynu ako prechodného paliva, ktoré spolu s hnedým uhlím malo vyplniť medzeru, ktorá vznikla kvôli

postupnému rušeniu atómových elektrární, a vydláždiť tak cestu pre veterné a solárne elektrárne. Zemný plyn predstavoval 15,3% vyrobenej elektriny v Nemecku v roku 2021 a 32% celkovej dodávky plynu pochádzajúceho z Ruska.

Nemecká situácia, založená na chybnej premise, že ruský plyn by mohol poskytovať stabilitu a bezpečnosť dodávok, ak nič iné, aspoň ako dočasné riešenie, mala za následok prehliadanie snahy Ruskej federácie o weaponizáciu (využitie nevojenských prostriedkov ako zbrane na dosiahnutie mocenských cieľov) energií a presadenie národných záujmov. Nemecko samozrejme nemusíme považovať za jediného (ani ideálneho) zástupcu zvyšku Európy. Niektorým krajinám sa už podarilo veľmi významne znížiť svoju závislosť na ruských energiách, avšak neúplne a príliš pomaly. Na druhej strane Rusko zostáva takmer kompletne závislé na Európe ako svojom primárnom trhu pre potrubný zemný plyn. Tento fakt podporujú čísla: v roku 2021, neskutočných 83% ruského exportu zemného plynu smerovalo do Európy, hoci dodávateľská základňa Európy je oveľa viac diverzifikovaná. Až 54% importu plynu nepochádza z Ruska, vrátane LNG z Nórska, Kataru a Alžírska alebo domácich zdrojoch ako sú plynové pole Groningen v Holandsku.

Napriek dlhodobým plánom Európskej únie zameniť zemný plyn za obnoviteľné zdroje energie, je neodškriepiteľný fakt, že sa táto energetická premena nedeje dostatočne rýchlo na to, aby mohli európske krajiny úplne znížiť spotrebu zemného plynu v krátkodobom horizonte, čo má za následok nevyhnutnosť hľadať alternatívnych dodávateľov zemného plynu, ako aj zrýchlenie krokov vedúcich k obnoviteľným zdrojom a zároveň veľmi aktuálne a veľmi mediálne vďačné šetrenie energiami v krajinách EÚ.

Hlavným princípom celého plánu je nahradiť ruské dodávky plynu sčasti zemným plynom vyprodukovaným v EÚ, sčasti importom cez potrubia z Azerbajdžanu (čo má tiež svoje politické úskalia, hlavne pre vzťah Azerbajdžanu s Tureckom a turecké geopolitické ambície) a Nórska a nakoniec aspoň momentálne obzvlášť dôležitými dodávkami LNG z Kataru, Alžírska a Spojených štátov. Dodávky LNG z USA do Európy už dokázali prekonať import ruského plynu potrubím – v júny dodalo Rusko iba 4,5 bcm, čiže tretinu toho, čo začiatkom roku 2021, kým americký LNG predstavoval 5,5 bcm v rovnakom období. Vďaka dodatočným opatreniam by sa mohol krátkodobo navýšiť tok LNG do Európy, čím by sa poskytla väčšia flexibilita a energetická bezpečnosť EÚ.

Ruské problémy so zemným plynom sú úzko prepojené s dlhodobými výzvami krajiny v rámci jej ekonomickej a politickej štruktúry, nemajú prechodný charakter a ich riešenie je komplikované. Rusko je obzvlášť zraniteľné vo viacerých doménach súvisiacich s exportom zemného plynu – samotná štruktúra ekonomiky založenej na komoditách, zásobovacie reťazce, technológie a v neposlednom rade aj reputácia ako spoľahlivého partnera, ktorý si plní svoje záväzky a kontrakty – toto všetko sa zhoršuje spolu so zhoršujúcou sa geopolitickou pozíciou Ruska.

Napriek Putinovej dezilúzii, že sa môže Rusko vrátiť do sovietskych čias sebestačnosti štátneho hospodárstva, faktom je, že Ruská ekonomika sa v priebehu posledných troch dekád stala vysoko globalizovaná a vo veľkom závisí od západných technológií a medzinárodných dodávateľských reťazcoch, čo ju robí zraniteľnejšou voči externým šokom a narušeniam. Model rastu ruského hospodárstva po rozpade Sovietskeho zväzu sa vo veľkom spoliehal na export surových tovarov s nízkou pridanou hodnotou naprieč hodnotovým reťazcom, bol však závislý od západných technológií pre ťažobný priemysel a od globálnych dodávateľských reťazcov – s podielom obchodu s tovarom a službami v HDP Ruska približne 46,1% v roku 2020.

Hoci sa pozornosť médií zameriava hlavne na ruskú weaponizáciu plynu vypnutím Nord Stream 1 (medzičasom sme boli svedkami podľa všetkého plánovaného poškodenia Nord Stream 1 aj Nord Stream 2, zatiaľ bez jasných dôkazov, ktorá strana ho spôsobila), vyznie ironicky, že síce sa EÚ zmieta v náročných časoch a stoja pred ňou obrovské výzvy nie len čo do energetickej bezpečnosti, obrovský – zrejme väčší – dopad to má na samotnú ruskú

ekonomiku, hlavne z dôvodu presunutia dodávateľských reťazcov zemného plynu preč z Európy, ktorá v súvislosti s touto komoditou predstavuje pre Rusko primárny trh. Kvôli sankciám znižuje Kremeľ predpoveď svojho už tak minimálneho exportu LNG – do roku 2026 bude export LNG menej ako 30,7 miliónov ton ročne. Ruské ministerstvo energetiky v septembri 2021 pôvodne predpokladalo, že sa objem exportu zvýši na 38 mil. ton v roku 2023 a 50,7 mil. ton v roku 2024 – ciele, ktoré už aj Kremeľ sám považuje za nedosiahnuteľné.

Na zmiernenie škôd spôsobených stratou európskeho trhu pre export zemného plynu sa podľa Putina má Rusko orientovať na iné trhy a vyhlásil "povorot na vostok" alebo otočku na východ. Rusko podľa neho musí diverzifikovať export a presmerovať ho na rýchlo rastúce trhy v Ázii. Tento krok predstavuje drastické otočenie, nakoľko 16,5 miliardy kubických metrov plynu dodaných do Číny minulý rok predstavovalo menej ako 10% z 170 miliárd kubických metrov zemného plynu poslaného Ruskom na európsky trh. Ak berieme do úvahy iba plyn cez potrubie, podiel zemného plynu z Ruska do Číny predstavuje iba 3,5%. Nedávna minulosť ukazuje, aké nepredvídateľné a zrejme aj naivné môže byť spoliehanie sa Ruska na všeobecný obrat na východ/Čínu. V roku 2014, keď boli po anexii Krymu voči Rusku prijaté relatívne mierne sankcie, Kremeľ predpokladal, že čínske firmy budú kupovať ruské aktíva, finančne podporovať ruské podniky a zdieľať s nimi technológiu a know-how – nič z tohto sa nestalo. Pre Čínu predstavuje Rusko malého obchodného partnera, kým USA sú stále obchodný partner číslo 1 a väčšina čínskych firiem nechce riskovať sankcie v prípade tajných obchodov s ruskými subjektmi. Čínske energetické podniky, ako dovozcovia čistej ropy a plynu, nemajú k dispozícii všetku potrebnú technológiu na servis a udržiavanie ruského sektora ropy a plynu. Ešte väčšie problémy pre spomínaný obrat na východ so sebou prináša logistika.

Za prvé, financovanie takýchto finančne nesmierne náročných projektov stavia Rusko do nevýhodnej situácie. Hlavné funkčné spojenie medzi Sibírou a Čínou "Sila Sibíri", ktoré stálo 45 miliárd dolárov a po celkovom dokončení bude mať dĺžku okolo 3 tisíc kilometrov, bolo v roku 2014 kompletne financované Čínou. Teraz však bremeno leží na Rusku, aby zafinancovalo nové projekty potrubí. Ako prípravu na masívne kapitálové výdavky bol Gazprom nútený pristúpiť k bezprecedentnému kroku, prvý krát v priebehu 30-tich rokov, a to k pozastaveniu vyplácania dividend a jeho akcie sa stali jedny z najmenej výkonných akcií na Moskovskej burze od začiatku invázie. K neľahkej situácii neprispieva ani fakt, že pri rokovaniach s Čínou Rusko očakávalo ceny primerané tým, ktoré účtovalo EÚ, avšak Čina vždy chcela ceny nižšie, ktoré by boli kompetitívne cenám uhlia a celkovo domácim cenám energií. Je treba uviesť, že prvé potrubie pre zemný plyn do Číny – Sila Sibíri 1 – je v prevádzke iba čiastočne. Pôvodne malo dodávať plyn z polí na východnej Sibíri, Kovykta a Čajanda, avšak kvôli technologickým problémom začalo produkciu iba druhé menované. Aj z dôvodu odstúpenia hlavných západných a čínskych firiem z Ruska po začatí invázie bude riešenie týchto problémov oveľa zložitejšie. Berúc do úvahy skutočnosť, že ázijská sieť potrubí pokrýva iba frakciu kapacity tej európskej a plánované projekty sú stále na roky vzdialené od plnej prevádzky, vyhliadka na navýšenie kapacity potrubí spájajúcich Rusko s Čínou je viac menej pochybná.

Za druhé, neexistuje žiadna prepojiteľnosť a tým pádom žiadna možnosť na presmerovanie dodávok plynu alebo kapitalizáciu cenovej arbitráže medzi ruským plynovodom Jamal a plynovými poľami na západnej Sibíri, ktorý exportuje do Európy a Stredného východu a poľami na východnej Sibíri, odkiaľ prúdi plyn do Číny. Navrhované riešenie – Sila Sibíri 2 – známe aj ako Altaj Transsibírsky plynovod, ktorý bol plánovaný ak spojenie týchto dvoch, bolo zastavené kvôli neustálym prieťahom zo strany Číny. To znamená, že plyn zo západnej Sibíri bude musieť z veľkej časti zostať v zemi. Okrem už spomenutého, existuje veľký rozdiel medzi exportnou LNG kapacitou Ruska a jeho exportom plynu cez plynovody. Dve LNG zariadenia napojené na západosibírsku plynárenskú sieť – Jamal a Vysotsk – dokážu exportovať objem 25 bcm. Celkový export zemného plynu z Ruska do Európy narástol až na 170 bcm, vrátane 15

bcm dodaných vo forme LNG. Už na prvý pohľad je jasné, že z technického hľadiska nie je možné dodať zostávajúce množstvo plynu do Číny alebo Indie bez veľkých nákladov a časovo náročného budovania transsibírskeho plynovodu, ktorý by spojil západnú časť Sibíri s východnou.

Ruská snaha o obrat na východ je teda oveľa komplikovanejšia, ako sa na prvý pohľad môže zdať, obzvlášť ak ide o zemný plyn. Nielen, že môže Rusko do Číny dodávať plyn iba z východnej Sibíri, otázkou je aj to, či Rusko pre Čínu predstavuje preferovaného dodávateľa. Čína zámerne diverzifikovala svoje dodávky LNG, využívajúc dodávateľov zo Strednej a Malej Ázie, ako aj USA, Austráliu a iných. V asymetrickom vzťahu medzi Čínou a Ruskom je to práve Rusko, ktoré je oveľa zraniteľnejšie, ak zohľadníme vyššie uvedené fakty.

Hoci sa Čína postupne snaží zbaviť využívania uhlia, aby naplnila svoje klimatické ciele a celkovo znížila environmentálne zaťaženie, má k dispozícii neustále narastajúce kapacity spätného splyňovania, čo predstavuje hrozbu pre ruský plyn prúdiaci cez plynovody a tlačí cenu ruského plynu smerom nadol, nakoľko Čína môže jednoducho dovážať LNG z celého sveta za cenu porovnateľnú – ak berieme do úvahy aj cenu za energetickú bezpečnosť – s ruským plynom. Konfrontácia so Západom znížila postavenie Ruska ako exportéra komodít nielen vo vzťahu s Čínou, ale aj s relatívne menšími partnermi z bývalého sovietskeho bloku, ako sú krajiny strednej Ázie. Ako príklad môžeme uviesť Kazachstan, ktorý sa pomalými, ale istými krokmi snaží odvrátiť od Ruska a jeho vplyvu (napr. v roku 2021 prešiel na latinku, v roku 2022 zrušili oslavu Dňa víťazstva a kazašský prezident Tokajev oponoval Putinovi na jeho vlastnej pôde na ekonomickom fóre v Petrohrade tento rok). Ruské odvetné opatrenia ako dočasné zastavenie prevádzky rusko-kazašského plynovodu Kaspian iba zvyšujú napätie a pobádajú Kazachstan, aby sa zameral viac na Čínu a Európu.

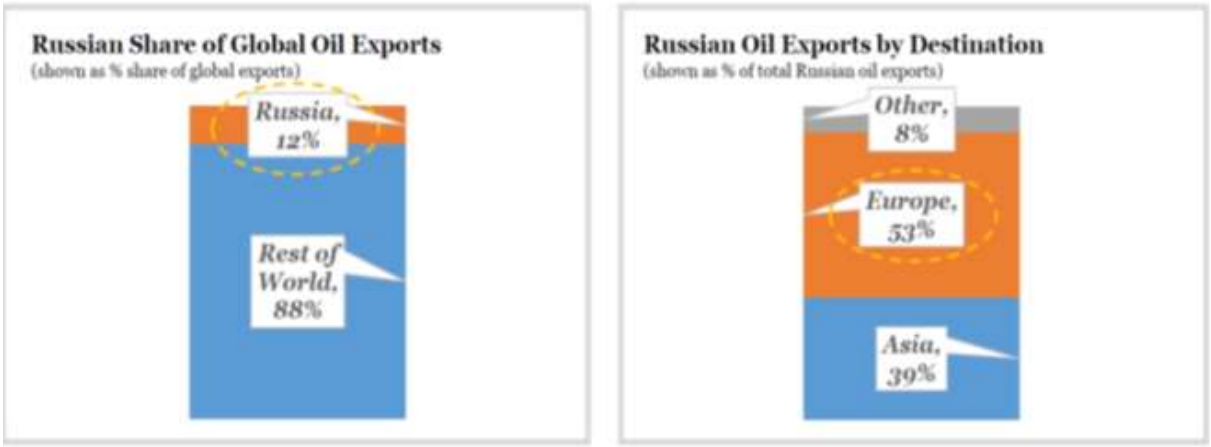
Ďalšou prekážkou ruského obratu na východ je skutočnosť, že čo sa týka exportu ropy a plynu, bolo Rusko značne závislé od západných technológií a know-how. Od prvých dohôd dodávok zemného plynu zo Sovietskeho zväzu v roku 1968, ktoré vo veľkom záviseli od kapacít nemeckých a rakúskych firiem, tak aj v súčasnosti sme mohli sledovať podobný problém pri stavbe plynovodu Nord Stream 2. Pôvodne išlo o spoločný podnik Gazpromu a piatich firiem z EÚ – Shell, E.ON, OMW, Wintershall a ENGIE. Po prijatí zákona na ochranu energetickej bezpečnosti Európy (PEESA) a následnom odstúpení holandsko-švajčiarskej firmy Allseas, projekt na dlhší čas zamrzol, hlavne z toho dôvodu, že Rusko nedisponovalo lodnou technikou na pokračovanie prác a trvalo vyše roka, kým bolo schopné upraviť svoje plavidlá na ukladanie potrubia.

Rovnako aj v prípade ruských aktivít v Arktíde hrozí, že bez podpory západných firiem, nebude schopné samo využiť potenciál plynových polí v arktickej oblasti. Okrem náročných podmienok, ktoré si vyžadujú špecifické vlastnosti stavebných materiálov použitých na budovách, celkový proces logistiky či vŕtania do zamrznutej zeme, výzvou sa stáva aj pritiahnutie talentovaných inžinierov do vzdialených, nehostinných oblastí.

2.2 ROPA

Asymetrický vzťah medzi Ruskom a jeho obchodnými partnermi môžeme opäť sledovať na trhu s ropou, kde Rusko potrebuje príjmy z exportu ropy oveľa viac, než "svet" ruskú ropu. Rusko je tretím najväčším producentom ropy. Údaje za január 2022 ukazujú, že vyprodukovalo 11,3 mb/d (miliónov barelov za deň), kým Saudská Arábia 12 mb/d a USA 17,6 mb/d. Okolo 88% jeho produkcie ropy – alebo približne 10 mb/d – pozostáva zo surovej ropy, z ktorej je 7,8 mb/d určeného na export. Približne 50-60% ruského exportu ropy išlo do európskych krajín OECD, kým iba 20% ide do Číny. Práve vývoz ropy je základom pre ruskú ekonomiku – oveľa viac, ako export plynu. V roku 2021 dosahovali celkové príjmy z exportu ropy 45% rozpočtových príjmov Ruska alebo inak povedané, trojnásobok príjmov z exportu zemného plynu. Nezávislí producenti ropy predstavujú menej ako 10% ruskej produkcie ropy

a úloha štátom vlastnených podnikov v priebehu času významne rástla úmerne snahám Ruska odkloniť sa od "hnedých polí" na západe Sibíri a viac sa zamerať na nové projekty na Jamalskom polostrove a v Arktíde. Sú to práve ropa a plyn, ktoré robia z Ruska relevantného hráča v svetovej ekonomike, napriek tomu, že produkuje iba 3% celosvetového HDP.



Obrázok 1: Export ruskej ropy
Zdroj: Yale Chief Executive Leadership Institute

Dlhodobá predpoveď vývoja ruskej produkcie ropy predpokladá hlboký prepad podnikov "na zelenej lúke" v projektoch plánovaných v arktickej oblasti a mierny prepad 2-3% ročne, čo sa týka hnedých polí. Predpokladá sa však, že tento prepad môže byť ešte strmší. Dôvody sú viaceré, jednak sa niektoré polia dostávajú do svojej poslednej produkčnej fázy a západné energetické firmy nie sú dostatočne nahradené čínskymi alebo indickými partnermi, čím klesá aj kvalita údržby. Aj samotné ministerstvo financií Ruskej federácie predpokladá, že by mohol v roku 2022 nastať pokles produkcie ropy medzi 9% – 17%, nakoľko západné sankcie a odchod medzinárodných ropných spoločností komplikujú ťažbu a znižujú dopyt.

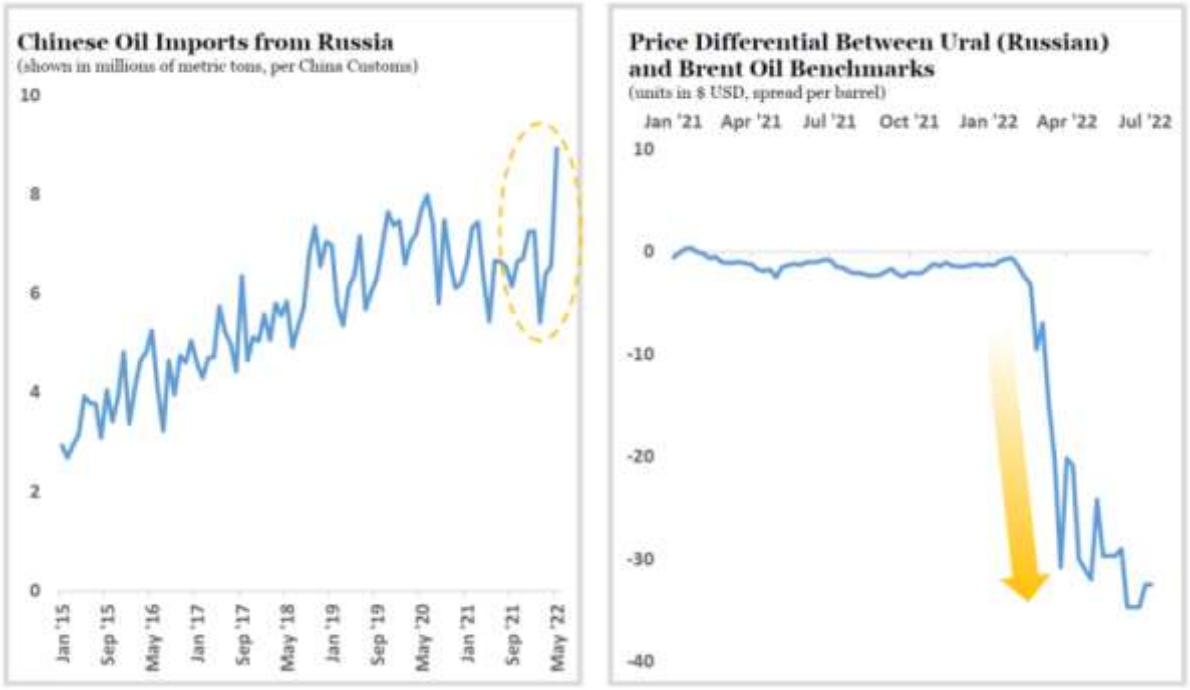
Následky úpadku ruských ropných polí sú kľúčovým faktorom pre budúcnosť Ruska ako energetickej a hlavne ropnej superveľmoci. Neschopnosť krajiny zvýšiť produkciu ropy by sa mohla ukázať ako ochromujúca. Nielen by tým stratila značnú časť svojho globálneho geopolitického vplyvu, ale kvôli nižšej produkcii a potenciálnemu poklesu ceny Uralskej ropy (aspoň relatívne voči iným typom), by ruský štátny rozpočet čelil trvalému rozpočtovému deficitu každý rok. Takéto dlhodobé pesimistické predpovede pre ruskú produkciu ropy boli popri neustálym správam o zvyšovaní cien v západných krajinách na úzadí mediálneho záujmu aj pozornosti odbornej verejnosti. Pochopiteľne, že negatívna zmena v krajinách EÚ si zaslúži pozornosť politikov, štátnych orgánov či médií, avšak bolo by nesprávne si myslieť, že Rusko sankciami netrpí viac.

Rovnako ako v prípade zemného plynu, aj s ropou sa Rusko snaží orientovať viac na východ. Nakoľko ide o ľahšie nahraditeľnú komoditu, predstavuje z pohľadu Ruska v rámci logistiky odklon na východ menej problémov, ako pri zemnom plyne. Už pred zavedením EÚ a USA sankcií sa západní dovozcovia a obchodníci vo veľkom vyhýbali nákupom ruskej ropy, a to nie len kvôli rizikám súvisiacim s reputáciou, ale aj kvôli ťažkostiam so zabezpečením poistenia a financovania dodávok, obzvlášť po tom, čo bola spoločnosť Shell kritizovaná za nákup zlacnenej ruskej ropy.

Minulý rok predstavovali dodávky ropy do Ázie 39%, avšak toto číslo určite narástlo v aktuálnom roku. Kremeľ síce od začiatku inváze nevydal žiadne štatistiky týkajúce sa exportu energií, z čínskych zdrojov však vieme indikovať, že Čína veľmi významne navýšila nákup ruskej ropy. Vyhrážky, že Rusko presmeruje väčšinu svojho exportu ropy pôvodne určeného

pre Západ, sú stále viac menej prázdne. Ako ukazujú výrobné kapacity krajín OPEC a potenciálne opatrenia na zníženie dopytu – Rusko je viac závislé od toho, aby západné krajiny "akceptovali" jeho ropu, ako je Západ od ruských dodávok. Je prakticky nemožné, aby boli Čína a India schopné prijať 6 mb/d v priebehu jedného roka. Po vrchole v mesiacoch apríl a máj, už údaje z júla 2022 ukazujú, že obe krajiny majú ťažkosti prijať novoobjavený prebytok ruskej ropy. Asymetrická vzájomná závislosť Ruska s jeho obchodnými partnermi dáva EÚ a Spojeným štátom významnú výhodu vo vyjednávaní.

Nemenej dôležitou skutočnosťou je, že Čína aj India nakupujú ruskú ropu s významnou zľavou (rozdiel 35$ medzi ropou Ural a Brent, hoci obe boli pred inváziou predávané za porovnateľné ceny). Rusko naďalej zostáva producentom s relatívne vysokými nákladmi v porovnaní s inými dôležitými producentami ropy, t. j. Saudskou Arábiou a USA, z toho dôvodu viac pocíti akýkoľvek maržový tlak.



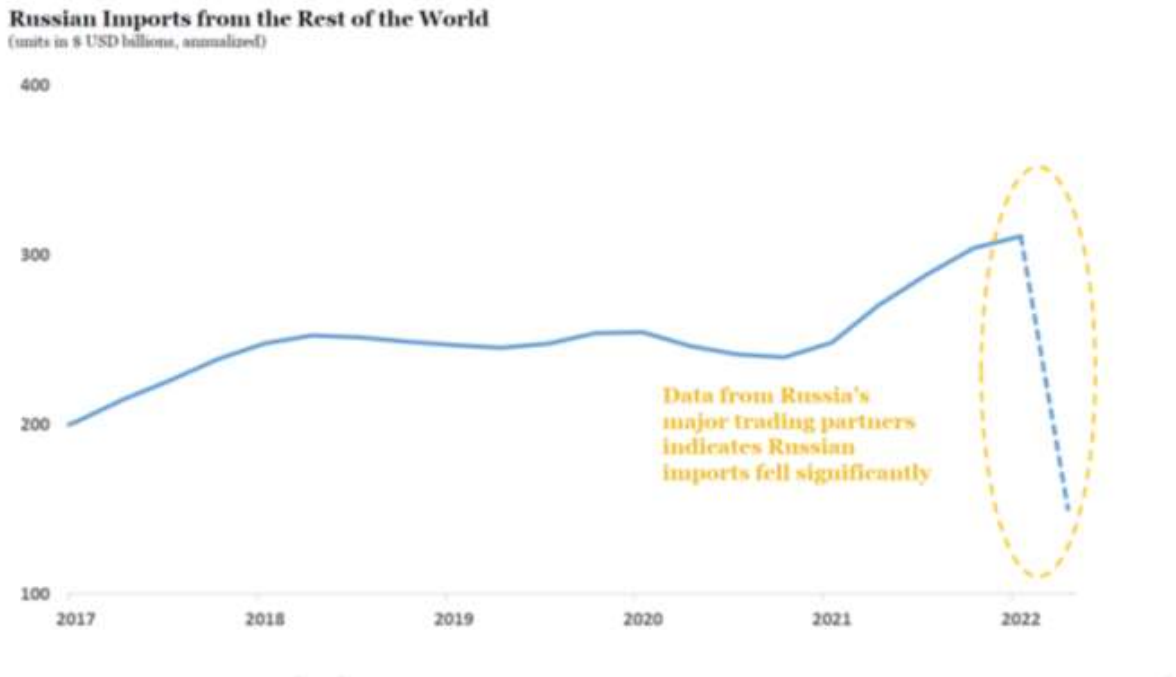
Obrázok 2: Čína nakupuje ruskú ropu za výhodnú cenu
Zdroj: Yale Chief Executive Leadership Institute

Situácia pre Rusko vyznieva značne odlišne od tradičných predstáv a prejavov. Nie len, že príjmy z ropy a plynu klesli medzimesačne v máji o viac ako polovicu (máj bol zároveň posledným mesiacom, kedy Kremeľ vydal pôvodne pravidelné štatistiky o exporte komodít), avšak pozícia Ruska ako strategického vývozcu komodít sa dramaticky zhoršila. Napriek vyhláseniam o odolnosti ruskej ekonomiky či propagande zo strany prezidenta Putina o tom, ako dokázali ruské energetické spoločnosti poraziť všetky výzvy vyplývajúce zo západných sankcií, skutočnosť je taká, že minimálne na ropnom trhu čelí Rusko existenčným výzvam. Jeho izolácia od západných krajín obrala Rusko o strategickú vyjednávaciu pozíciu voči Číne a Indii, kupcom, ktorí sú notoricky zameraní na cenu a ktorí udržiavajú blízky vzťah aj s ostatnými dodávateľmi komodít. Už v minulosti nemali problém využiť situáciu krajiny, na ktorú boli uvalené sankcie, čo sme mohli sledovať pri jednaniach Číny s Iránom či Venezuelou, kde sa Číne podarilo získať obrovskú zľavu na ropu. Ešte dôležitejším faktorom vplývajúcim na situáciu Ruska ako vývozcu ropy a zemného plynu je situácia s technológiami a prerušenými vzťahmi s medzinárodnými partnermi. Bez nich má totiž Rusko významne sťaženú situáciu a

šancu na využitie svojich obrovských rezerv ropy a plynu, hlavne na Sibíri a v Arktíde. Z krátkodobého pohľadu to znamená, že Rusko stráca nielen kľúčové príjmy z daní, ale aj globálnu kredibilitu a spoľahlivosť, ako členská krajina aliancie OPEC+ a je odkázané na nákupy Číny a Indie, ktorým musí poskytovať významné zľavy. Zo strednodobého pohľadu povedie ruská technologická nevýhoda a neschopnosť prístupu na globálne trhy takmer určite k dramatickému poklesu produkcie ropy – podľa niektorých scenárov na približne 6 miliónov barelov za deň v priebehu pár rokov – hlavne kvôli absencii medzinárodných investícií, technológií a know-how.

3 POKLES RUSKÉHO IMPORTU ILUSTRUJE SLABINU ASYMETRICKÝCH VZŤAHOV RUSKA V RÁMCI GLOBÁLNEJ EKONOMIKY

Princíp vzájomnej asymetrickej závislosti - a zhoršujúca sa strategická pozícia Ruska – vplýva na všetky aspekty vzťahov Ruska v rámci globálnej ekonomiky. V predchádzajúcej časti sme sa bližšie venovali role Ruska ako vývozcu komodít, nakoľko práve ich export má obrovský význam pre financovanie rozpočtu ruskej vlády a tým pádom financovanie vojenských akcií, avšak nemenej dôležitá je aj úloha importu v rámci ruskej domácej ekonomiky. Dovoz predstavuje približne 20% ruského HDP a domáca ekonomika vo veľkom závisí od importu medzi odvetviami a medzi hodnotovým reťazcom, napriek Putinovej predstave o sebestačnosti.



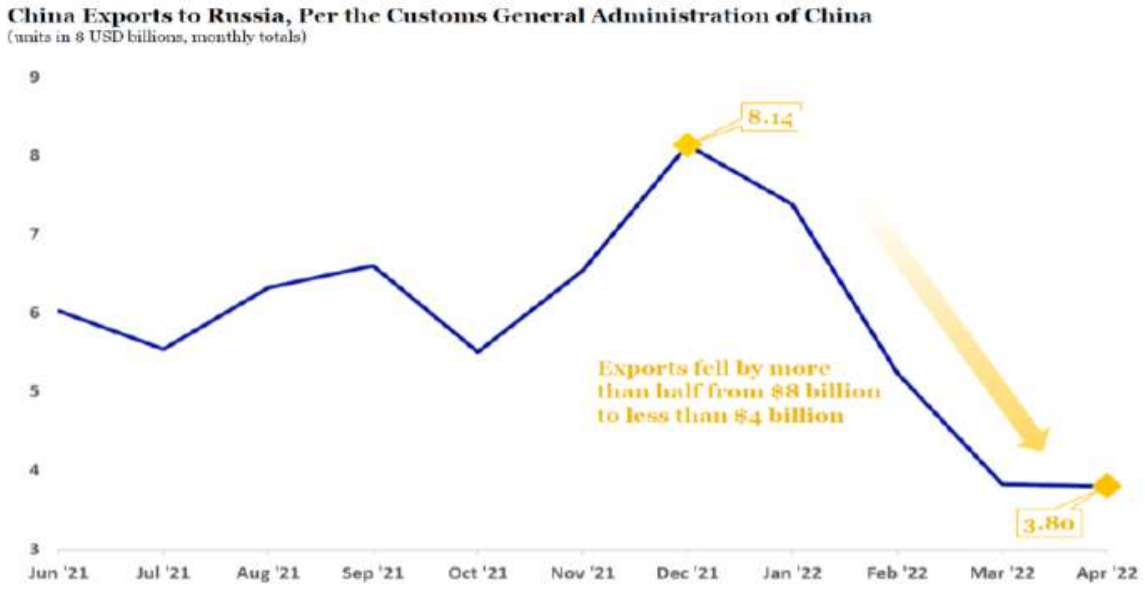
Obrázok 3: Ruský import
Zdroj: Yale Chief Executive Leadership Institute

Ruskému importu sa mimo samotnej krajiny nedostáva takej pozornosti pre niekoľko dôvodov. V prvom rade, hoci je kľúčový pre domácu spotrebu a výrobu a tým pádom životy bežných Rusov, nepredstavuje významný zdroj príjmov. Tarify získané z importov predstavujú iba malú časť ruského rozpočtu a väčšina ekonómov, politikov a analytikov sa zameriavala viac na hlavný zdroj ruských príjmov – export komodít – ako na ruský import, hoci je dôležitý vnútroštátne.

Druhým dôvodom je fakt, že výskumníci opäť narážajú na nedostatok dostupných údajov. Rosstat (Federálna služba štátnej štatistiky Ruskej federácie) pozastavil zverejňovanie aktuálnych dát o importe a Rusko už viac nevydáva ani podzložky obchodných údajov. Z uvedeného vyplýva, že akékoľvek odhady aktuálneho dovozu do Ruska sa musia vykonať využitím obchodných údajov obchodných partnerov Ruskej federácie. Po tretie, to málo pozornosti, ktoré bolo venované dovozu sa disproporčne zameralo iba na úniky informácií. Import do Ruska bezpochyby neklesol na nulu. Podľa Sonnenfeld et al. (Sonnenfeld et al, 2022), zoznam firiem, ktoré obmedzili svoje pôsobenie v Rusku stále zahŕňa niekoľko stoviek firiem označených ako "F" – čo znamená, že obchodujú v Rusku ako predtým, neovplyvnené odchodom vyše tisícky svojich globálnych partnerov. Keď sa už ruskému importu venuje akákoľvek pozornosť, je to zvyčajne o firmách, ktoré pokračujú vo svojom biznise v Rusku a importujú do Ruska aj naďalej. Hoci je aj tento pohľad dôležitý, selektívne príklady firiem, ktoré neprestali dodávať tovar do Ruska jednoducho nemôžu zachytiť celkový pohľad.

Pravdou je, že import do Ruska v mesiacoch nasledujúcich od začiatku invázie výrazne klesol. Prehľad obchodných údajov od top obchodných partnerov Ruska – nakoľko Kremeľ aj tieto údaje prestal zverejňovať – naznačuje, že ruský import klesol o vyše 50% v prvom mesiaci invázie. Napriek zatajovaniu zo strany vlády, už aj ruská Centrálna banka priznala určitý pokles.[1] V prvých dňoch invázie a odchodu západných firiem z ruského trhu zaznievali hlasy, ktoré pochybovali o akomkoľvek vplyve takéhoto kroku na ruskú ekonomiku, nakoľko mali za to, že uvoľnené miesta budú okamžite vyplnené čínskymi firmami, ktoré by si nenechali ujsť príležitosť obchodovať v Rusku. Po uplynutí niekoľkých mesiacov môžeme povedať, že skutočnosť bola dosť odlišná. V skutočnosti, podľa aktuálnych mesačných zverejnených údajov Všeobecnej colnej správy Čínskej ľudovodemokratickej republiky, ktorá má k dispozícii detailné obchodné údaje s členením exportu podľa jednotlivých obchodných partnerov, čínsky export do Ruska klesol o 50% od začiatku roka do apríla, čo predstavovalo pokles z vyše 8 miliárd dolárov mesačne na konci roka 2021 na menej ako 4 miliardy dolárov v apríly 2022. Tieto informácie sa zároveň zhodujú s pozorovaním niekoľkých čínskych bánk, ktoré stiahli všetok svoj kredit a financovanie z Ruska takmer ihneď po začatí invázie. Išlo o banky ako ICBC, New Development Bank a Asian Infrastructure Investment Bank, ale aj energetický gigant Sinochem, ktorý pozastavil všetky investície a spoločné podniky v Rusku.

[1] https://www.cbr.ru/eng/press/event/?id=12765



Obrázok 4: Čína podľa svojich oficiálnych údajov znižuje export do Ruska
Zdroj: Bloomberg

Výzvy pre ruskú ekonomiku sa dajú sledovať aj cez selektívne oficiálne štatistiky, ktoré zatiaľ Rosstat vydáva, hlavne cez mesačné údaje spotrebiteľských cien. Nielen, že oficiálny index spotrebiteľských cien Ruska dosiahol približne 20% infláciu v mesiacoch po invázii – čím dosiahol najvyššie úrovne od finančnej krízy koncom 90-tych rokov minulého storočia – ale po bližšom pohľade na rôzne sektory je podľa indexu spotrebiteľských cien vidno, že situácia je ešte horšia, ako sa predpokladalo. Odvetvia, ktoré závisia najviac od medzinárodných dodávateľských reťazcov, sú konfrontované s infláciou dosahujúcou až 40-60% - vrátane technológií, ubytovacích a gastro služieb či západných automobilov. Množstvo z tovarov odkázaných na medzinárodné dodávateľské reťazce bolo po začiatku invázie takmer nemožné kúpiť. Pred inváziou bolo v Rusku mesačne predaných priemerne 100 000 automobilov, tento počet však klesol na štvrtinu. Najaktuálnejšie údaje indikujú, že v júni bolo v Rusku predaných iba 27 000 automobilov.

Zoznam zahraničných automobiliek, ktorých predaj klesol o viac ako 90% v medziročnom porovnaní v júni 2022 je dlhý: Lexus, Volvo, Fiat, Porsche, Toyota, Land Rover, Škoda Auto, Volkswagen, Mitsubishi, Volkswagen Vans, Audi, Jaguar, Suzuki, Nissan, Lifan, Renault, Ford, Hyundai, Opeli, Infiniti, Lada, Mazda, Kia, Peugeot, Citroen, Subaru, Jeep, Geely, UAZ.

Žiadny segment ruskej populácie nebol ušetrený domácemu ekonomickému chaosu. Automobilový priemysel je iba jeden z mnohých príkladov, kde sa spotreba zastavila. Podobnú situáciu zažíva napr. obchod so smartfónmi.

3.1 EXODUS FIRIEM, KAPITÁLU A TALENTOV

Popri zhoršujúcej sa obchodnej pozícii a zápasu na poli domáceho hospodárstva dochádza aj k dlhodobému narušeniu ekonomickej situácie a výhľadov do budúcna. Deje sa to hlavne z troch dôvodov:

1) odchod firiem z Ruska

2) odliv zahraničného kapitálu a investícií
3) imigrácia a odchod talentovanej a vzdelanej pracovnej sily

Hoci tieto javy nie sú zachytené v oficiálnych ruských štatistikách ani v niektorých analýzach ruskej ekonomiky, degradácia budúcej základne produktivity ruského hospodárstva a neschopnosti odraziť sa od aktuálnych zlých pozícií narastá spolu s predlžovaním sankcií.

Podľa Sonnenfeld et al. (Sonnenfeld et al, 2022), ak vezmeme hodnotu investícií (v Rusku) vyše tisícky zahraničných firiem, ktoré odišli z krajiny od začiatku inváze, celková hodnota presahuje 600 miliárd amerických dolárov – sumu zodpovedajúcu približne 40% ruského HDP. Tieto firmy zamestnávali celkovo vyše jeden milión domácich zamestnancov. V priebehu troch mesiacov sa tak zvrátili tri desaťročia, kedy sa ruská ekonomika po rozpade Sovietskeho zväzu snažila integrovať do svetovej a kedy ruskí obchodníci a politickí lídri mali snahu dotiahnuť zahraničné investície do Ruska.

Samozrejme to neznamená, že ruský HDP za noc klesne o 40%. Množstvo z tisícky firiem, ktoré obmedzili svoje prevádzkové činnosti v Rusku, sú stále v procese likvidácie svojich prevádzok, čo znamená, že potrvá mesiace ak nie roky, aby sme mohli naplno vyhodnotiť dopad tohto kroku. Ďalšie z týchto firiem už previedli alebo predali svoje ruské prevádzky domácim subjektom, čo znamená, že síce z dlhodobého hľadiska im bude možno chýbať západná technologická a finančná podpora a know-how a ich situácia sa môže zhoršovať, z toho krátkodobého však budú naďalej do určitej miery prevádzkyschopné a nemôžu byť okamžite odpísané z ruského HDP. Existujú aj firmy, ktoré pokračujú v niektorých činnostiach v Rusku aj naďalej, zatiaľ čo svoje ďalšie činnosti pozastavili, takže akýkoľvek negatívny vplyv týchto firiem na ruský HDP by bol iba čiastočný. Je nemožné zachytiť celkový ekonomický dosah odchodu zahraničných firiem z ruského trhu, nakoľko množstvo z najzničujúcejších následkov budeme môcť sledovať až s odstupom niekoľkých rokov, avšak už z vyššie spomenutého je zrejmé, že sa ruská ekonomika bude musieť zaoberať dramatickými transformáciami, ktorých riešenie nebude vôbec jednoduché.

Nie je prekvapením, že s odchodom zahraničných firiem z Ruska úzko súvisí aj "odliv mozgov", nakoľko talentovaní, vzdelaní Rusi húfne opúšťajú krajinu. Nie je možné presne určiť, koľko Rusov od začiatku invázie permanentne opustilo krajinu, avšak odhady hovoria o počte okolo 500 000 osôb.

3.2 NEUDRŽATEĽNÉ FINANČNÉ STIMULY A INTERVENCIE KREMĽA AKO ZNÁMKA SLABOSTI EKONOMIKY

Po odchode veľkého počtu firiem a zavedení sankcií nielen zo strany EÚ a USA, ale aj ďalších štátov sveta, malo množstvo západných ekonómov a politikov nerealistické očakávania, že sa ruská ekonomika zrúti alebo dôjde k finančnej kríze. Sankcie iba málokedy vedú k finančnej kríze alebo ekonomickému kolapsu. Sú skôr stavané tak, aby dlhodobo štrukturálne oslabili národnú ekonomiku jej izoláciou od globálnych trhov. V našom článku sme ukázali, že dopad odchodu zahraničných firiem a zavedenie niekoľkých balíčkov sankcií na ruskú ekonomiku sa rovnali takmer katastrofe (strata kompetitívnosti ruskej ekonomiky a zároveň zhoršujúca sa vnútorná štrukturálna slabosť). Avšak dôvodom, prečo nedochádza k rýchlejšiemu kolapsu ruskej ekonomiky – ako niektorí predpokladali – bola bezprecedentná a neudržateľná fiškálna a monetárna odpoveď iniciovaná Kremľom.

Pomocou masívnych a neudržateľných vládnych intervencií bola ruská vláda schopná dočasne podoprieť ruskú ekonomiku a menu. Rubeľ bol podľa niektorých meraní ešte v júni 2022 najvýkonnejšou menou na svete. Ihneď po začiatku invázie vyskočil výmenný kurz rubľa k doláru z 75 na 110, avšak Kremeľ okamžite oznámil prísny súbor kontroly kapitálu, pozostávajúci z nasledovných krokov:

- všeobecný zákaz pre občanov posielať peniaze na bankové účty v zahraničí,

- zákaz transferu cudzích mien,
- pozastavenie výberu hotovosti z dolárových bankových účtov vo výške nad 10 000$ na osobu,
- poverenie pre všetkých vývozcov na zamenenie 80% ziskov zahraničnej meny na ruble,
- pozastavenie priamej konverzie doláru pre jednotlivcov s bankovými účtami denominovanými v rubľoch,
- pozastavenie domácich pôžičiek v cudzích menách,
- pozastavenie predaja dolárov medzi tuzemskými bankami,
- mandát, aby firmy platili zahraničný denominovaný dlh v rubľoch,
- podpora jednotlivcov vymeniť doláre za ruble z patriotických dôvodov.

Tieto reštriktívne kontroly kapitálu viedli okamžite k tomu, že bolo prakticky nemožné pre Rusov legálne nakúpiť doláre alebo sa aspoň dostať k majoritnej časti svojich depozitov v dolároch, zatiaľ čo dochádzalo k umelému nárastu dopytu po rubľoch prostredníctvom nútených nákupov zo strany hlavných exportérov.

Rusko sa už nachádza v strategicky nevýhodnej pozícii a bude čeliť zrejme poklesu príjmov za ropu a plyn v nasledujúcich rokoch. Akýkoľvek pokles príjmov alebo vyvezených objemov za tieto dve komodity by okamžite vytvoril tlak na vládny rozpočet. V prípade, že by k tomu došlo, bude zaujímavé sledovať, akým spôsobom by Putin financoval rôzne nové avizované programy. Keď prišlo v minulosti k poklesu príjmov za ropu a plyn, bol Putin schopný použiť netransparentné fondy vo výške 600 miliárd dolárov devízových rezerv a Národného fondu bohatstva, avšak existujú náznaky, že aj tieto zdroje sú pod tlakom.

Najzreteľnejšou výzvou pre Putinove fondy je skutočnosť, že z týchto 600 miliárd dolárov v devízových rezervách, ktoré sa naakumulovali z príjmov za ropu a plyn, až polovica je zmrazená a mimo dosah spriatelených krajín, nakoľko sa nachádzajú v USA, Európe a Japonsku. Objavili sa už aj hlasy volajúce po tom, aby boli tieto finančné prostriedky použité na povojnovú obnovu Ukrajiny.

ZÁVER

Názory, že ruská ekonomika vráti úder alebo sa jednoducho so všetkým poľahky vysporiada a prežije sankcie bez najmenšieho poškodenia, nie sú objektívne. Skutočnosť je taká, že akoukoľvek metrikou a na akejkoľvek úrovni ruská ekonomika kolíše a ak chce Európa a jej spojenci dosiahnuť spoločný cieľ, nie je čas na nejednotnosť a zaváhanie. Zároveň však bude dôležité nenechať sa strhnúť situáciou a vidinou spravodlivého víťazstva. V globalizovanom svete by nemalo byť nikomu na prospech, ak sa iná krajina zmieta v ekonomickom chaose. Čím skôr sa konflikt skončí, tým skôr sa budeme môcť sústrediť na obnovu a rozvoj.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

COUNCIL OF THE EU. 2022. *Russia´s military aggression against Ukraine: EU agrees new sectoral measures targeting Belarus and Russia.* [online].
Dostupné na internete: https://www.consilium.europa.eu/en/press/press-releases/2022/03/09/russia-s-military-aggression-against-ukraine-eu-agrees-new-sectoral-measures-targeting-belarus-and-russia/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%25u2019s+military+aggression+against+Ukraine:+EU+agrees+new+sectoral+measures+targeting+Belarus+and+Russia

COUNCIL OF THE EU. 2022. *Russia´s aggression against Ukraine: EU adopts sixth package of sanctions.* [online].
Dostupné na internete: https://www.consilium.europa.eu/en/press/press-releases/2022/06/03/russia-s-aggression-against-ukraine-eu-adopts-sixth-package-of-sanctions/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%25u2019s+aggression+against+Ukraine%3a+EU+adopts+sixth+package+of+sanctions

ISIDORE, CH., LIAKOS, CH. 2022. *Russia moves to seize hundreds of planes from foreign owners.* [online].
Dostupné na internete: https://edition.cnn.com/2022/03/16/business/russia-aircraft-seizure/index.html

MARSH, S., CHAMBERS, M. 2022. *Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens.* [online].
Dostupné na internete: https://www.reuters.com/business/energy/germanys-scholz-halts-nord-stream-2-certification-2022-02-22/

SONNENFELD, J.A. et al. 2022. *Business Retreats and Sanctions Are Crippling the Russian Economy*. 2022.

STEIN, J., WHALEN, J. 2022. *Biden aides explore rarely used sanctions weapon against Russia*. [online].
Dostupné na internete: https://www.washingtonpost.com/us-policy/2022/03/24/russia-economy-sanctions/

THE WHITE HOUSE. 2022. *Executive Order on Prohibiting Certain Imports and New Investments with Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine.* [online].
Dostupné na internete: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/08/executive-order-on-prohibiting-certain-imports-and-new-investments-with-respect-to-continued-russian-federation-efforts-to-undermine-the-sovereignty-and-territorial-integrity-of-ukraine/

EU External Action Service, Press remarks by High Representative Josep Borrell,

European Commission, EU sanctions against Russia following the invasion of Ukraine, 2022. Dostupné na internete: EU sanctions against Russia: factsheet.

EU adopts fifth round of sanctions against Russia over its military aggression against Ukraine, Council of the European Union. 9. marec 2022a. Dostupné na internete: **Press release**

EU adopts fifth round of sanctions against Russia over its military aggression against Ukraine, Council of the European Union. 8. apríl 2022b. Dostupné na internete: **Press release**

Európska komisia: EK navrhuje pravidlá týkajúce sa konfiškácie majetku páchateľov trestnej činnosti a oligarchov, 2022. Dostupné na internete:https://europskenoviny.sk/2022/05/27/ek-navrhuje-pravidla-tykajuce-sa-konfiskacie-majetku-pachatelov-trestnej-cinnosti-a-oligarchov/

Official Journal of the European Union. L 63, Vol. 65, 2. marec 2022. Dostupné na internete: Publications Office (europa.eu)

Official Journal of the European Union. L 87 I, Vol. 65, 15. marec 2022a. Dostupné na internete: Official Journal of the European Union, L87 I,

Official Journal of the European Union. L 110, Vol. 55, 8. apríl 2022b. Dostupné na internete: L110/55,

Russia's military aggression against Ukraine: EU agrees new sectoral measures targeting Belarus and Russia. Council of the European Union, 2022. Dostupné na internete: Press release

Russia's aggression against Ukraine: EU adopts sixth package of sanctions. Council of the European Union, 2022c Dostupné na internete: Press release, (3. jún 2022).

Russia's aggression against Ukraine: the EU imposes restrictive measures on Viktor and Oleksandr Yanukovych. Council of the European Union, 2022d. Dostupné na internete: Press release, (4. august 2022).

Ing. Marek HARGAŠ
Letná 5, Bratislava
hargasmarek@hotmail.com

KONCEPT „HUMAN SECURITY“ AKO DETERMINANT VNÚTORNEJ BEZPEČNOSTI ŠTÁTU

THE CONCEPT OF "HUMAN SECURITY" AS A DETERMINANT OF THE INTERNAL SECURITY OF THE STATE

Ladislav HOFREITER

ABSTRACT

National security is affected on the one hand by its sensitivity, or resistance to external influences and forces, but especially the internal nature of the state, namely the socio-political cohesion of the state, ensuring human, civil rights, and legitimate needs of citizens.

The increase poverty, inequalities, discrimination, injustice, feelings of grievance among the population threaten the internal security, order and stability of the state. The feeling of threat to religious or other identity, together with the feeling of wrong from material lack and unavailability of health care, are important sources of social conflicts. Moreover, social conflicts have a high potential to change internal security.

In this article, we want to analyse how the implementation of the Human Security concept can affect the level of internal security of the state.

Keywords: internal security, Human Security, threat.

ÚVOD

Bezpečnosť sama o sebe je často vnímaná predovšetkým ako stav bez vojny alebo jej hrozby. V tomto kontexte je bezpečnosť definovaná ako schopnosť odolať ozbrojenému útoku zo zahraničia. Tradičné chápanie bezpečnosti je teda spojené s hodnotením hrozieb prevažne vojenského charakteru, s obranou štátu, koalície, s vojenským presadzovaním národných a koaličných záujmov, s elimináciou hrozby jadrovej vojny ap.

Bezpečnosť štátu, jeho politickú a sociálnu stabilitu, integritu a nezávislosť môžu ovplyvňovať rôzne činitele. V závislosti od paradigmy skúmania bezpečnosti ako takej, prípadne od paradigmy skúmania národnej bezpečnosti, sú používané rôzne prístupy.

V doterajších prácach, zaoberajúcich sa skúmaním národnej bezpečnosti, sme predstavili dva prístupy(Hofreiter, L., 2014, Hofreiter, L., 2015). Podľa prvého je národná bezpečnosť ponímaná ako ochrana národa a územia pred fyzickým útokom z vonka, ako schopnosť štátu brániť sa proti vojenským útokom zvonka. Znamená to takú situáciu, v ktorej nehrozí štátu žiadny útok zvonka, resp. ak ku ta-kému útoku dôjde, bude úspešne eliminovaný obrannými schopnosťami štátu.

Druhý prístup spočíva v zaistení vnútorného poriadku, stability politického systému, hospodárskeho rozvoja, sociálnej súdržnosti , ochrany národných kultúrnych hodnôt, sektorov kritickej infraštruktúry, bezpečnosti občanov i sociálnych skupín. Tento kontext, akcentujúci vnútornú bezpečnosť (Internal Security) je súhrn vnútorných bezpečnostných podmienok, legislatívnych noriem a opatrení, ktorými štát zabezpečuje demokraciu, ekonomickú prosperitu, bezpečnosť občanov, ako aj presadzovanie právnych a morálnych noriem.

Rovina vnútornej bezpečnosti a stability štátov zohráva významnú rolu v danom geopolitickom priestore. Ide najmä o to, aby priestor stability a bezpečnosti v regióne bol

garantovaný predovšetkým vnútornou stabilitou krajiny, založenej na fungujúcom demokratickom politickom a pluralitnom systéme, na vláde zákona, rešpektovaní ľudských práv a osobných slobôd, fungujúcej trhovej ekonomike a sociálnom systéme. Paradigmou pre posudzovanie úrovne národnej bezpečnosti sa tak môže stať namiesto štátocentrickej paradigmy koncept ľudskej bezpečnosti (Human Security).

1 KONCEPT „HUMAN SECURITY“

Ľudská bezpečnosť (Human Security) je v najširšom význame definovaná ako sloboda od strachu a sloboda od nedostatku. Stotožňovaná je s ochranou človeka pred takými hrozbami, ako je hlad, nemoci, represie, kriminalita, i ochranou pred pôsobením neočakávaných a škodlivých vplyvov na život človeka (prírodné a iné katastrofy). V podstate ide o zaistenie podmienok pre prežitie a dôstojný život človeka v súčasnosti a podmienok jeho pretrvania a rozvoja do budúcnosti. Výrazným príspevkom k premene konceptualizácie bezpečnosti smerom k ľudskej bezpečnosti boli práce Kodanskej školy (najmä Barryho Buzana) a školy tzv. tretieho sveta (napríklad Mohameda Ayooba a Amitava Acharyiu) z počiatku osemdesiatich rokov (Hofreiter, L., Zvaková, Z., 2019). Obe školy spochybnili dominantnú pozíciu štátu, pretože zdôrazňovali, že:

- referenčným objektom nie je len štát, ale i ľudský jedinec;
- vedľa vojenských hrozieb existuje celá paleta ďalších hrozieb, ktoré môžu výrazne poškodiť, respektíve oslabiť bezpečnosť jedinca (i štátu), ako je napríklad zhoršovanie stavu životného prostredia, nedostatočný rozvoj a zaostalosť spoločnosti, kriminalita, organizovaný zločin, či nedostatok surovín (vrátane potravín a pitnej vody);
- činnosť, resp. nečinnosť, či zlyhanie štátu sa môže stať zdrojom hrozieb pre jedinca (sociálnu skupinu) i širšie bezpečnostné prostredie.

V roku 1994 sa po prvýkrát v správe OSN o ľudskom rozvoji (Human Development Report 1994) objavil pojem „ľudská bezpečnosť“ (Human Security), ktorý bol spojený predovšetkým so zaistením bezpečnosti človeka ako indivídua. Tento koncept bezpečnosti spočíva v oslobodení človeka od strachu (*Freedom from Fear*) a oslobodení od nedostatku (*Freedom from Want*). Garantovanie týchto dvoch slobôd, spolu so zaistením slobody slova, slobody vyznania a práva na dôstojný život tvorí piliere pre zaistenie bezpečnosti človeka, a tým vlastne aj štátu. Vznik konceptu Human Security je spojený s dvoma súbormi podmienok:

- Riešenie problému ľudskej bezpečnosti je potrebné ako reakcia na zložitosť a vzájomnú súvislosť starých a nových bezpečnostných hrozieb – od chronickej a pretrvávajúcej chudoby až po etnické násilie, obchodovanie s ľuďmi, klimatické zmeny, zdravotné pandémie, medzinárodný terorizmus a náhly hospodársky a finančný pokles. Takéto hrozby majú tendenciu presúvať sa nad rámec tradičných predstáv o bezpečnosti, ktoré sa zameriavajú len na vonkajšie vojenské agresie.
- Zaistenie bezpečnosti ľudí si vyžaduje komplexný prístup, ktorý využíva širokú škálu nových príležitostí na riešenie takýchto hrozieb integrovaným spôsobom. Ohrozenie bezpečnosti ľudí nie je možné riešiť iba konvenčnými mechanizmami. Vyžaduje si nový prístup, ktorý uznáva prepojenia a vzájomné závislosti medzi rozvojom, ľudskými právami a národnou bezpečnosťou.

Východiskami pre formulovanie konceptu Human Security sa stali tri práva:

- individuálne základné práva, ako právo na život, slobodu a hľadanie šťastia, ktoré by malo byť chránené medzinárodným spoločenstvom,

- právo na bezpečnosť ľudí - civilistov a nekombatantov- v ozbrojených konfliktoch , na ochranu pred genocídou a na trestanie vojnových zločinov
- právo na priaznivé životné podmienky a ochranu pred ekonomickými, politickými, environmentálnymi a inými hrozbami.

Koncept Human Security spája v sebe prvky bezpečnosti, práv a rozvoja. V podstate ide o interdisciplinárny koncept, ktorý vykazuje tieto charakteristiky (Comission...,2003):

- je zameraný na ľudí,
- je multisektorový,
- je komplexný,
- je kontextovo špecifický,
- je zameraný na prevenciu.

Keďže ide o koncept zameraný na bezpečnosť ľudí, stavia jednotlivca do „centra analýzy“. V dôsledku toho zvažuje širokú škálu podmienok, ktoré ohrozujú prežitie, životné podmienky a dôstojnosť človeka, a identifikuje hranicu, pod ktorou je ľudský život neúnosne ohrozený.

Zaistenie bezpečnosti ľudí je založené na multisektorovom chápaní hrozieb. Koncept Human Security preto zahŕňa širšie chápanie hrozieb súvisiacich napríklad s ekonomickou, potravinovou, zdravotnou, environmentálnou, osobnou, komunitnou a politickou bezpečnosťou. Prehľad je uvedený v tabuľke 1.

Komplexita súčasného bezpečnostného prostredia je charakteristická aj vzájomnou previazanosťou a multiplikáciou bezpečnostných hrozieb. Z toho vyplýva, že bezpečnosť ľudí nemožno riešiť izolovane prostredníctvom parciálneho riešenia hrozieb a bezpečnosti v jednotlivých sektoroch. Riešenie a zaistenie ľudskej bezpečnosti je garantované jedine komplexným prístupom, vyžadujúcim potrebu kooperatívnych a multisektorových reakcií na identifikované, resp. prognózované bezpečnostné hrozby naprieč sektormi Human Security.

Kontextovo špecifická koncepcia ľudskej bezpečnosti rešpektuje, že štruktúra a intenzita hrozieb a bezpečnostná situácia referenčných objektov sa značne líšia v rôznych prostrediach. Preto i reakcia na hrozby a riešenie bezpečnosti referenčných objektov musí zohľadňovať špecifiká a kontext daného prostredia a podmienok v ňom.

Napokon, pri riešení rizík a základných príčin hrozieb je realizácia konceptu Human Security zameraná na prevenciu, na včasnú identifikáciu príčin a predpokladov vzniku bezpečnostných hrozieb. Realizácia tejto charakteristiky konceptu Human Security je podmienená znalosťou kauzálneho mechanizmu. Zo zákona kauzality vieme, že každý jav je vyvolaný určitou príčinou alebo súborom príčin. Existencia, nastúpenie alebo pôsobenie príčiny ešte neznamená vyvolanie, nastúpenie následku. Samotné nastúpenie je podmienené istými podmienkami. V procese kauzálneho pôsobenia príčiny vystupujú ako nezávisle premenné, následok je závisle premenná. Podmienky predstavujú sprostredkujúce premenné a až tieto vyvolávajú, resp. umožňujú vznik následku (závisle premennej). Prevencia potom znamená:

- zabránenie vzniku príčin,
- pôsobenie na podmienky, resp. vytvárať také tak, aby tieto pôsobili retardačne, teda aby vytvorili bariéru medzi príčinou a jej možného následku – hrozby,
- znížiť zraniteľnosť a zvýšiť odolnosť referenčného objektu vo vzťahu k potenciálnym i reálnym hrozbám jeho bezpečnosti.

Tabuľka 1 Štruktúra hrozieb v sektoroch Human Security

Sektor	Referenčné objekty	Agenda	Hrozby
Ekonomická bezpečnosť	Jednotlivci, zamestnanci , sociálne odkázaní,	Prístup k zamestnaniu, istému príjmu, spravodlivému platu, bývaniu, službám	Nezamestnanosť, materiálna deprivácia, chudoba a sociálne vylúčenie
Potravinová bezpečnosť	Všetci ľudia	Fyzická a ekonomická dostupnosť potravín	Nedostatok , nedostupnosť potravín, chudoba, hlad, hladomor
Zdravotná bezpečnosť	Všetci ľudia	Prístup k liečbe a liečebnej prevencii, zdravá výživa, čistá voda.	Nedostupnosť základnej zdravotnej starostlivosti, choroby, infekcie, pandémie, nebezpečné potraviny, vodný stres
Environmentálna bezpečnosť	Všetci ľudia, ľudstvo ako celok, ekosféra, biosféra	Politiky a prax zamerané na udržateľnosť ekosystému a biosféry, ochrana vody, pôdy a vzduchu.	Degradácia životného prostredia, znečisťovanie vody, pôdy, emisie, odlesňovanie, priemyselné havárie
Politická bezpečnosť	Všetci ľudia	Ochrana a garantovanie ľudských práv, občianskych slobôd, volebného práva, sloboda vyjadrenia názoru,	Politicída, porušovanie ľudských a občianskych práv, nedemokratické režimy, zlyhávajúce a nefunkčné štáty.
Osobná bezpečnosť	Všetci ľudia	Ochrana pred násilím, zločinom, ochrana života a majetku, ochrana nekombatantov vo vojne, zaistenie osobnej slobody.	Fyzické násilie, kriminalita, terorizmus, vojny, domáce násilie, detská práca, obchodovanie s ľuďmi, otrocká práca,
Societárna bezpečnosť	Jedinci, sociálne skupiny, národy a národnosti, náboženské skupiny, menšiny	Ochrana sociálnych skupín, vrátane národnostných, náboženských , etnických skupín, ochrana tradičných kultúrnych identít,	Asimilačná politika, migrácia, vplyv silnejších štátov, vplyv cudzích kultúr, nerešpektovanie náboženský a kultúrnych práv.

Zdroj: Vlastné spracovanie

2 NOVÉ HROZBY „HUMAN SECURITY“

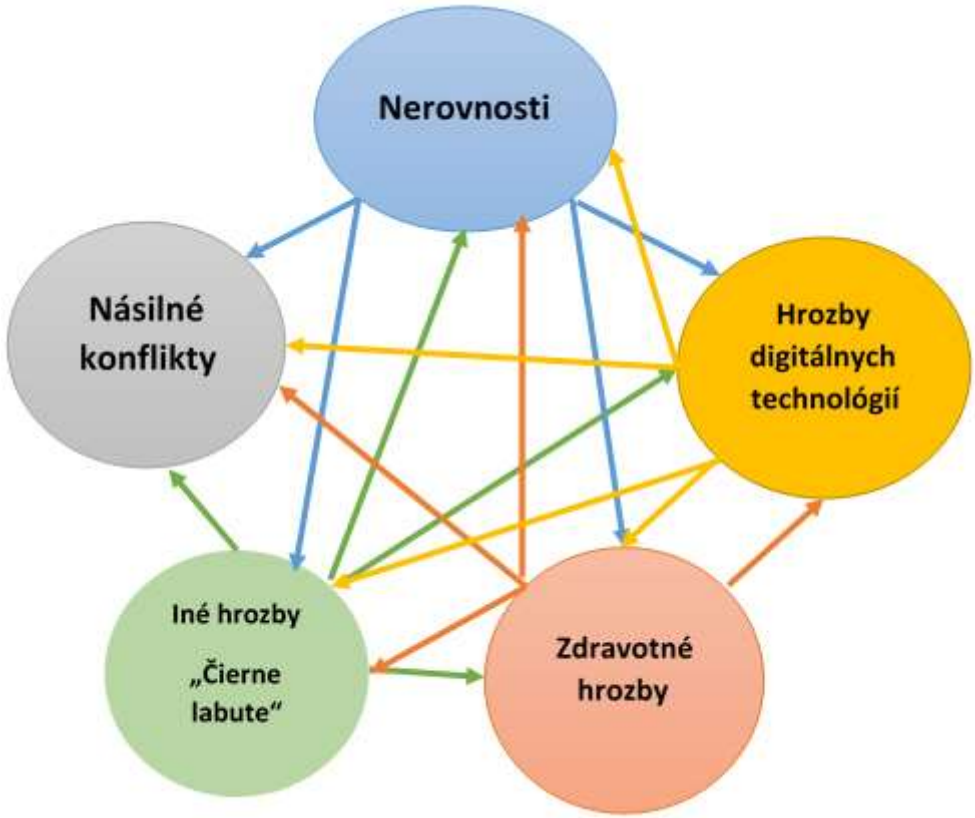
Koncept Human Security bol vypracovaný a prijatý pred takmer tromi desaťročiami. V roku 1994 OSN definovala nové ponímanie bezpečnosti pre 21. storočie. Podľa predloženej definície bezpečnosť :

- to nie je len bezpečnosť štátu, je to bezpečnosť ľudí,
- to nie je bezpečnosť dosiahnutá prevahou zbraní, ale bezpečnosť dosiahnutá ako výsledok rozvoja,

- to nie je len jednoducho bezpečnosť štátu, to je predovšetkým bezpečnosť každého človeka vo svojom dome či na svojom pracovisku,
- to nie je len obyčajná ochrana pred konfliktmi medzi štátmi, je to hlavne a najmä ochrana pred konfliktmi medzi národmi.

Napriek očakávaniu a optimizmu z postupnej erózie hrozby vojenskej konfrontácie medzi blokmi štátov sa začiatkom milénia objavili nové generácie hrozieb, ktoré sú globálne, systémové a vzájomne prepojené. Táto nová realita je silným objektívnym dôvodom, prečo miera neistoty a pocitu ohrozenia v ľuďoch narastá. Ukázalo sa, že dosiahnuté úspechy v oblasti blahobytu – predtým koncipované ako rozvojové úspechy – nestačia na to, aby boli vyriešené všetky otázky bezpečnosti ľudí. Nové hrozby sa prejavujú aj v prostredí, v ktorom hmotná núdza nie je dominantná.

Report *New threats to human security in the Anthropocene* (UNDP, 2022) upozorňuje na nové hrozby, súvisiace s digitálnymi technológiami, násilnými konfliktami, nerovnosťou medzi skupinami a nedostatkom v súčasných systémoch zdravotnej starostlivosti (obr.1.) Do tohto spektra hrozieb sme doplnili kategóriu nových hrozieb, tzv. „Čierne labute“.



Obrázok 1 Štruktúra nových hrozieb ľudskej bezpečnosti.
Zdroj: Vlastné spracovanie podľa „New threats...“

2.1 HROZBY DIGITÁLNYCH TECHNOLÓGIÍ

Pokrok v digitálnych technológiách bol kľúčom k pokroku v mnohých dimenziách ľudského rozvoja (od prístupu k zdravotníckym a vzdelávacím službám až po podporu schopností a spôsobilostí spojených s prístupom k informáciám a komunikácií). Na druhej strane nesú so sebou značné riziká. Niektoré aspekty nových informačných a digitálnych technológií pretvárajú sociálne a rodinné interakcie, pracovné podmienky a voľnočasové aktivity. Koncentrácia moci medzi niektorými novými globálnymi hráčmi v oblasti

digitálnych technológií a rýchlosť odvíjajúcich sa zmien vytvárajú výzvy pre tvorcov národných politík. Niektoré z týchto zmien majú negatívne vedľajšie účinky na mnohé sektory ľudskej bezpečnosti. Zneužívanie moci a politickej nadvlády môže byť výsledkom koncentrácie kontroly nad informáciami, môže vyvolať obmedzovanie slobôd, prehlbovanie nerovností a šírenie informácií, ktoré podporujú polarizáciu.

V Bezpečnostnej stratégii Slovenskej republiky 2021 je na spektrum digitálnych hrozieb reagované v dvoch smeroch: ako kybernetický úrok a hybridné hrozby.

Kybernetické útoky majú potenciál nielen ohroziť chod štátu a plnenie jeho funkcií, spôsobiť významné ekonomické škody, ale aj narušiť spoločenskú stabilitu a poriadok v štáte. Digitálne technológie a informačné systémy môžu byť využité aj na ovplyvňovanie verejnej mienky, polarizáciu spoločnosti, rozsievanie nedôvery voči štátu, na propagáciu extrémizmu a vyvolávanie nevraživosti medzi sociálnymi skupinami v štáte. Každá z týchto hrozieb, materializovaná a realizovaná prostredníctvom digitálnych technológií má vysoký konfliktogénny potenciál s dopadom na vnútornú bezpečnosť štátu, ale aj na jeho akceptáciu v medzinárodnom prostredí.

2.2 NÁSILNÉ KONFLIKTY

Konflikt predstavuje určitú kvalitu vzájomných vzťahov medzi jednotkami sociálneho prostredia- aktérmi, ktorými môžu byť jednotlivci, sociálne skupiny, štáty alebo koalície štátov, prejavujúce sa v ich úsilí o presadenie svojich potrieb, dosiahnutie svojich záujmov a cieľov na úkor a proti vôli svojich oponentov, resp. ktoré sú protichodné so záujmami protistojacej strany (Hofreiter, L., 2008, s.33). Konflikt býva spravidla s určitou formou násilia, nátlaku, potom tieto konflikty charakterizujeme ako násilné konflikty.

V násilných konfliktoch uplatňujú strany (aktéri) konfliktu najmä priame, zjavné násilie, ktoré je možné identifikovať ako *fyzické násilie, fyzické útoky, fyzické týranie, bitku, pouličné nepokoje, ničenie majetku, vandalizmus, mučivé zabíjanie, ozbrojené akcie povstaleckých, teroristických či gerilových skupín, alebo, v najkrajnejšej forme ako vojny*. Toto násilie sa obyčajne prejavuje ako vyústenie iných, menej viditeľných foriem násilia (najmä štrukturálneho násilia). Pri tejto forme násilia môžeme jednoznačne identifikovať aktérov – útočníkov, i obete. Priame násilie často používajú aj utláčané, diskriminované, marginalizované a vylučované sociálne skupiny, ktoré nemajúc iných možností, keď už inej cesty niet, používajú násilie ako legitímny nástroj na vyjadrenie protestu.

Pre násilné konflikty sú charakteristické ľudské obete, vysoké materiálne straty, deštrukcia infraštruktúry štátu, masívne porušovanie ľudských práv a občianskych slobôd. Sú sprevádzané morálnou a mravnou degradáciou obyvateľstva, rozvrátením alebo narušením sociálneho a politického systému štátu, environmentálnou degradáciou priestoru. Konflikty prinášajú so sebou aj veľa ďalších problémov: chudobu, hlad a choroby, ľuďom v oblasti konfliktov sa nedostáva žiadna alebo len nekvalitná zdravotnícka starostlivosť. V dôsledku konfliktov sa mnoho ľudí dostáva do pozície utečencov (*refugees*), alebo mnoho ľudí býva vnútorne presídlených (*internally displaced persons*).

Každý násilný vnútorný konflikt sťažuje alebo znemožňuje normálne ekonomické aktivity a hospodársky rozvoj štátu. Nie je to len v dôsledku zastavenia alebo zníženia produkcie, či hospodárskej izolácie oblasti konfliktu, ale aj v dôsledku úbytku ľudských zdrojov, tzv. „intelektuálnej genocídy“, keď krajinu konfliktu opúšťa nielen pracovná sila, ale aj odborníci na riadenie ekonomiky a štátu, ale aj učitelia, zdravotnícky personál a pod.

2.3 NEROVNOSTI

V reálnom živote pozícia človeka nie je rovnoprávna, nie každý má rovnaký prístup k materiálnym a kultúrnym zdrojom pre zaistenie svojich potrieb, vrátane zaistenia potreby bezpečnosti. V sociálnom prostredí je prítomná nerovnosť sociálnych jednotiek – jednotlivcov i skupín (Holmquist, G. 2012) Keď hovoríme o nerovnosti, základnou otázkou je : nerovnosť *medzi čím, medzi kým?*

V rámci štruktúry sociálneho prostredia[1] štátu vzniká rozvrstvenie danej populácie do usporiadaných tried (Sorokin, P. 2009). Rozvrstvenie populácie môže byť :

- **ekonomické** , podľa ekonomického statusu (bohatí, chudobní,...),
- **politické**, podľa podielu na moci (vrstva vládnuca, vláda, vrstva ovládaných, občania, stupne orgánov a inštitúcií politickej moci),
- **profesijné**, podľa spoločenského uznania vykonávaného povolania,
- **kultúrne,** podľa príslušnosti k dominantnej kultúre, alebo k subkultúram či marginalizovaným skupinám,
- **národnostné, etnické,** podľa príslušnosti k národnostným či etnickým skupinám,
- **religiózne**, podľa príslušnosti k náboženstvám a cirkvám,
- **rodové,** podľa príslušnosti k skupine podľa pohlavia,
- **vekové,** podľa príslušnosti k skupinám podľa veku,
- **podľa pracovnej aktivity,** teda podľa príslušnosti do predproduktívnej, produktívnej, poproduktívnej skupiny.

V takto rozvrstvenom sociálnom prostredí štátu môžu vznikať *vertikálne nerovnosti,* ktoré súvisia s pozíciou sociálnej skupiny (jednotlivca) v hierarchickej štruktúre prostredia štátu (skupiny), zatiaľ čo *horizontálna nerovnosť* ukazuje na rozdiely medzi priemermi vo vnútri rôznych skupín.

Nerovnosti medzi skupinami majú rôzne proporcie:

- ekonomické nerovnosti sa vzťahujú sa na rozdiely v prístupe k majetku, platom a príležitosti zamestnania;
- sociálne nerovnosti sa vzťahujú na rozdiely v prístupe k sociálnym službám;
- politické nerovnosti vyjadrujú rozdiely v politických príležitostiach a podiele na moci;
- kultúrne nerovnosti vyjadrujú rozdiely v možnostiach a podmienkach zachovávania jazyka, náboženstva a obyčají.

Treba tiež objasniť, v čom spočíva nerovnosť: dominantnými disparitami v sociálnom prostredí je napríklad: príjmová nerovnosť, majetková nerovnosť, politická nerovnosť, kultúrna nerovnosť, rodová nerovnosť, nerovnosť v dostupnosti sociálnych služieb, práva, adekvátneho zamestnania, atď.

Nerovnoprávna pozícia človeka je dôsledkom ekonomickej, politickej i profesijnej **stratifikácie**, ktorá sa vyvíjala s rozvojom spoločnosti. Zaistenie základných životných i kultúrnych potrieb, prístup k dostatku zdravých potravín, k lekárskej starostlivosti, vzdelaniu, primeraný finančný príjem za prácu – to nezáleží vždy len od vôle človeka, ale od jeho pozície v spoločnosti, od jeho ekonomického, politického, sociálneho i profesijného statusu. Rovnako je to aj v prípade zaistenie ochrany a bezpečnosti človeka pred násilím[2],

[1] Sociálny priestor je určený univerzom ľudskej populácie, roztriedenej do sociálnych skupín. Súhrn všetkých sociálnych skupín spolu so súhrnom všetkých pozícií každej z nich tvorí systém sociálnych súradníc, ktoré umožňujú jednoznačne určiť sociálnu pozíciu každého človeka. Sociálny priestor je tak viacrozmerný priestor, čím viacej je populácia podelená, čím je zložitejšie štruktúrovaná, tým viacej rozmerov má.

[2] Myslíme násilie fyzické štrukturálne i kultúrne. Pozri : Hofreiter, L. 2008, s.34-42.

v dostupnosti a vymožiteľnosti práva, v rešpektovaní jeho osobnej, kultúrnej, náboženskej národnostnej, ale i sexuálnej identity a integrity. Iné sú možnosti človeka z vyšších spoločenských vrstiev, iné sú možnosti človeka nezamestnaného, chudobného a marginalizovaného. Práve vysoký stupeň sociálnych nerovností, chudoba a vylúčenie sú jednou z príčin asymetrie ľudskej bezpečnosti.

Analyzujúc kvantitatívne i kvalitatívne stránky nerovností môžeme konštatovať nasledujúce (Hofreiter, L., 2008):

- Nelegitímnosť sociálnych nerovností v očiach časti verejnosti znižuje pocit ich občianskej záväznosti, lojality a konformity vo vzťahu k spoločenskému celku. Takéto pocity sa stávajú často významným krimonogénnym a konfliktogénnym činiteľom.
- Nerovnomerný vývoj, sociálne nerovnosti, nemožnosť uspokojiť základné existenčné potreby, zvyšujú frustráciu a riziko agresívneho správania. V prostredí chudobných a sociálne vylúčených budú jedni chudobní bojovať s inými chudobnými, predovšetkým o prístup k obžive a teda o prežitie.
- Nerovnomernosť vývoja, ďalšie prehlbovanie rozdielov a zvyšovanie chudoby môže vyvolať nespokojnosť v zaostávajúcich oblastiach, a môže byť zdrojom ohrozenia bezpečnosti nielen vo vnútornom prostredí štátu, ale i v širšom prostredí až v globálnom rozsahu.
- Problémy skupinových identít inklinujú k násilným konfliktom, keď sa prekrývajú s ekonomickými a politickými nerovnosťami,
- Politickí (náboženskí) vodcovia využívajú frustráciu a depresiu z nedostatku spojením s niektorou z identít ako nástroj na mobilizáciu podporovateľov a sympatizantov. Vyvolanie pocitu ohrozenia náboženskej alebo inej identity spolu s pocitom krivdy z materiálneho nedostatku sa stáva významným konfliktogénnym činiteľom.

2.4 ZDRAVOTNÉ HROZBY

Hrozby vzniku a šírenia nových chorôb, epidemie i pandémie (SARS, HIV, COVID-19), nekontrolované šírenie epidémií a nákaz zvierat a dobytka (epi-zootie) sú jedným významných činiteľov, ovplyvňujúcich ľudskú bezpečnosť. Šírenie nových chorôb sa stáva globálnym problémom, pretože v tomto prípade administratívne hranice skutočne nepredstavujú žiadnu prekážku. Existuje tu akási analógia so šírením organizovaného zločinu či počítačových vírov.

Vplyv týchto činiteľov na vývoj bezpečnostnej situácie súvisí s kvalitou a dostupnosťou zdravotníckej starostlivosti najmä pre tých najchudobnejších, či už v krajinách tretieho sveta, alebo aj pre sociálne marginalizované skupiny vo vyspelých krajinách. Výdobytky lekárskych vied nemajú rovnaký vplyv na predlžovanie ľudského života pre všetky vrstvy, v mnohých krajinách sa nedarí znižovať detskú úmrtnosť, tuberkulóza sa začína objavovať aj v európskych krajinách, chorobu AIDS sa nedarí eliminovať a naopak, objavujú sa nové, nebezpečnejšie mutácie prenosných chorôb.

Účinky koronavírusu SARS-CoV-2, vyhláseného za pandémiu v marci 2020, sa rozšírili takmer na každého na svete a zaútočili na všetky dimenzie ľudského rozvoja. Väčšina ekonomík zaznamenala stagnáciu a zmenšovala sa rekordným tempom a deti nemohli fyzicky navštevovať školu. Výskyt tejto pandémie odhalil obmedzenia zdravotných systémov na národnej a medzinárodnej úrovni, najmä rozšírený nedostatok koordinácie na mnohých úrovniach, čo sa výraznejšie odrazilo vo veľkých rozdieloch v prístupe k vakcíne medzi krajinami a vo využívaní vakcín v mnohých krajinách, medzi nimi i na Slovensku. Zameranie zdravotného systému na riešenie pandémie znížilo dostupnosť zdravotnej starostlivosti v neinfekčných prípadoch, nevykonávali sa potrebné , ale i preventívne liečebné

zákroky, čo sa nutne prejavilo aj v úmrtnosti na necovidové ochorenia. Pandémia COVID-19 spôsobila výrazné zvýšenie mier úmrtnosti na Slovensku, už v roku 2020 prekročil počet zomretých hodnotu 1 000 úmrtí na 100-tisíc obyvateľov a v roku 2021 sa zvýšil až na 1 350. V SR zomrelo v roku 2021 vyše 73-tisíc ľudí, čo bolo o 20-tisíc osôb viac ako v rokoch pred pandémiou, pričom podiel zomretých na COVID-19 bol evidovaný 20%. (https://slovak.statistics.sk)

Vysoká infekčnosť nových chorôb, a v tomto prípade COVID-19, si vyžiadala podstatné obmedzenie sociálnych kontaktov, dodržiavanie karanténnych opatrení, obmedzenie pohybu osôb a uzavretie mnohých prevádzok, čo malo nielen ekonomický dopad, ale sa prejavilo aj v psychickom zdraví obyvateľstva. Obmedzenie sociálnych kontaktov a izolácia výrazne ovplyvňovali predovšetkým mladých ľudí, ktorí trpia zvýšenou nervozitou, depresiami, úzkosťou, hnevom a osamelosťou, pocity osamelosti a opustenosti sa negatívne prejavovali aj na duševnom zdraví starších a najmä osamelých ľudí.

Pandémia COVID-19 ukázala zraniteľné miesta sociálneho, ekonomického i zdravotného systému a mala závažné dôsledky pre zdravie, hospodársky pokrok, dôveru vo vládu a sociálnu súdržnosť.

2.5 INÉ HROZBY

Okrem hrozieb, uvedených v tabuľke 1, môžu na bezpečnosť ľudí vplývať aj iné, doposiaľ neidentifikované hrozby. K takým patria:

- Zlyhanie svetového systému
- Udalosti nazývané „Čierne labute“.

2.5.1 ZLYHANIE SVETOVÉHO SYSTÉMU

Dnešný moderný svet je zložitý systém, zložitejší než kedykoľvek predtým. Tento vzájomne technologicky previazaný systém , majúci globálny rozmer, má neobmedzené množstvo stupňov voľnosti – príležitostí, možností, volieb, čo zároveň spôsobuje jeho nestabilitu. Vzájomné prepojenosť a závislosť zložitej infraštruktúry nevyhnutnej pre zabezpečenie životného štýlu postmoderného človeka ho robí zároveň i zraniteľným voči vplyvu neočakávaných (?) a udalostí, ktoré môžu vzniknúť v jednom zo sektorov infraštruktúry (v jednom z podsystémov spoločnosti) a spôsobiť tak otras v celom systéme. Môžu kedykoľvek nastať udalosti prekvapivého charakteru, ktoré môžu vyvolať chaos, napáchať škody a mať potenciálne obrovský dopad na ľudský život. Tieto „extrémne udalosti“ nazýva **John Casti** „*udalosti X*“ (Casti, 2012, s.7), a sama udalosť X je výsledkom zložitosti, ktorá sa vymkla kontrole (Casti, 2012, s. 62).

Politológ **Thomas Homer-Dixon** v knihe *The Upside of Down (Svetlá stránka pádu)* (Homer-Dixon, 2006) na margo súčasného sveta píše, že dôsledkom rastu počtu väzieb jeho subsystémov vzniká taká tesná prepojenosť, že porucha v jednej časti otrasie celým systémom. Identifikuje päť „*tektonických stresov*“, ktoré môžu zvýšiť riziko kaskádového zrútenia životne dôležitých systémov. Jav, ktorý nazýva "*synchrónny zlyhanie*", môže spôsobiť:

- energetický stres z narastajúceho nedostatku konvenčnej ropy;
- ekonomický stres z narastajúcej globálnej ekonomickej nestability a prehlbujúcej sa príjmovej nerovnosti medzi bohatými a chudobnými;
- demografický stres z nerovnomerného rastu populácie v bohatých a chudobných krajinách, z rastu počtu mestskej populácie a populácie v chudobných krajinách;

- stres zo zhoršovania životného prostredia, znečisťovania pôdy, vody, lesov a zhoršovania podmienok rybolovu;
- klimatický stres zo zmien v zložení zemskej atmosféry.

Riziká vyplývajúce zo zložitosti súčasného sveta a jeho bezpečnostného prostredia spočívajú najmä v emergentom správaní sa svetového systému, ktoré vzniká v dôsledku interakcií jeho podsystémov a prvkov, ako i z nedostatku znalostí o vlastnostiach, ktoré vzniknú ako dôsledok týchto interakcií.

Zložitosť spoločenských systémov a ich vzájomných vzťahov narastá, rovnako sa vyhrocujú i konkurenčné vzťahy, čo môže viesť ku kolapsu niektorých systémov, neschopných obstáť v konkurencii iných systémov.

Narastenie spektra ohrození znižuje schopnosť adekvátneho reagovania na ne, v konfrontácii s narastajúcou kvantitou a kvalitou hrozieb sa zvyšuje zraniteľnosť spoločenských systémov.

Zložitosť spoločenských vzťahov v svetovom systéme vyžaduje primeranú zložitosť systému riadenia; avšak zložitosť môže viesť k dysfunkcii riadiacich štruktúr a vzniku globálneho chaosu.

Zachovanie hranice medzi voľnosťou a reguláciou (riadením) spoločenských vzťahov, potrieb a záujmov je veľmi krehké. Zrejmé je to v prípade zaistenia potreby bezpečnosti a zároveň i slobody a voľnosti.

Napriek zdokonaľujúcim sa schopnostiam prognózovať budúci vývoj, vždy bude dochádzať k udalostiam, ktoré sme nepredpokladali. Je to preto, že súčasný svet je zložitý, nestabilný a neusporiadaný systém a v každom bode trajektórie jeho vývoja môže dôjsť k odchýlkam od očakávaného stavu, objavenia sa extrémnych udalostí, strategických šokov, ktoré môžu dramaticky zmeniť podmienky života ľudí a ich bezpečnosť.

2.5.2 UDALOSTI „ČIERNE LABUTE“

Udalosť typu „Čierna labuť“[3] (*Black Swan*) je mimoriadne zriedkavá udalosť s vážnymi následkami. Nedá sa predvídať, hoci sa niekedy vyskytujú názory, že udalosti, ktoré nastali, mohli byť predvídateľné.

Charakteristickými atribútmi udalostí typu Čierna labuť sú (Hofreiter,L., Kubíková, Z. 2020):

- neočakávané, prekvapivé objavenie sa (nastúpenia) udalosti,
- katastrofické škody a dramatický dopad (účinok) na verejnú morálku,
- po ich odznení je možné ich objasniť, identifikovať ich príčiny a metódy pôsobenia.

Za udalosti typu Čierna labuť považujeme, vzhľadom na ich vplyv na ľudskú bezpečnosť, najmä:

- všetky druhy teroristických útokov,
- útoky na objekty typu „mäkký cieľ“ (Soft Target)4
- prípady masovej streľby (*mass shooting*)[5].

Uvedené udalosti môžu spôsobiť katastrofické škody, resp. straty na životoch, či poškodenie zdravia ľudí. Napriek snahe o ich predvídanie, využívanie spravodajských

[3] Teóriu vyvinul Nassim Nicholas TALEB v roku 2001, aby vysvetlil pôsobenie neočakávaných udalostí veľkého rozsahu a ich dôsledkov.

[4] Za objekty typu mäkký cieľ (Soft Target) sa považujú objekty a priestory s hromadným výskytom osôb, napr. obchodné domy, veľké zhromaždenia ľudí, kultúrne, náboženské alebo športové podujatia.

[5] Za udalosť typu Mass Shooting (hromadná streľba) sa považuje incident, pri ktorom sú minimálne tri alebo štyri obete násilia so zbraňou (okrem strelca) v krátkom časovom období.

informácií a metód modelovania budúcich stavov bezpečnostnej situácie, nemôže vždy zabrániť týmto udalostiam . Možnosti výskytu týchto udalostí vyvoláva v občanoch pocit strachu, možného ohrozenia ich vlastnej bezpečnosti alebo bezpečnosti ich blízkych. Znemožňuje to dosiahnutia oslobodenia sa od strachu, najmä pri pobyte v inkriminovaných objektoch alebo udalostiach.

ZÁVER

Rovina vnútornej bezpečnosti a stability štátov zohráva významnú rolu v danom geopolitickom priestore. Ide najmä o to, aby priestor stability a bezpečnosti v regióne bol garantovaný predovšetkým vnútornou stabilitou štátov, založenej na fungujúcom demokratickom politickom a pluralitnom systéme, na vláde zákona, rešpektovaní ľudských práv a osobných slobôd, fungujúcej trhovej ekonomike a sociálnom systéme.

Koncept ľudskej bezpečnosti je nevyhnutným predpokladom pre vytvorenie podmienok na vnútornú bezpečnosť a stabilitu štátu. Zaistenie oprávnených potrieb občanov a sociálnych skupín, vytvorenie takých podmienok , aby mohli žiť dlhý a zdravý život, získať primerané vzdelanie, mať prácu a spravodlivú mzdu, možnosť užívať politické slobody a ľudské práva, cítiť sa bezpečne vo svojom dome i na ulici, nemať strach o svoje deti, ako i mať istotu, že príležitosti a podmienky, ktoré majú ľudia dnes, budú mať i v budúcnosti , znamená skutočné oslobodenie od strachu a oslobodenie od nedostatku.

Pokiaľ človek, občan, ale aj sociálne skupiny nadobudnú tieto slobody a istoty, odstráni sa tým možnosť vnútorných sociálnych, národnostných či etnických konfliktov, a tým vlastne bude garantovaná vnútorná bezpečnosť a stabilita štátu. A tým aj bezpečnosť v regionálnom kontexte.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

CASTI, J.2012. *Události X. Možné scénáře kolapsu dnešního složitého světa*. Praha: Management Press, Praha, 2012. ISBN 978 8072 6120 55

Commission on Human Security.2003: *Human security now : protecting and empowering people.* [online] New York, 2003. Dostupné na Internete: https://digitallibrary.un.org/record/503749

HOFREITER, L. 2008. *Teória a riešenie konfliktov.* Liptovský Mikuláš : AOS, 2008. ISBN 978-80-8040-347-8

HOFREITER, L. 2012. Asymetria národnej a medzinárodnej bezpečnosti . In : *Národná a medzinárodná bezpečnosť 2012*.Zborník vedeckých a odborných prác. Liptovský Mikuláš: AOS, 2012, s. 143-152. ISBN 978 – 80-8040-4508-5

HOFREITER, L. 2014. Vnútorné činitele národnej bezpečnosti. In: *Národná a medzinárodná bezpečnosť 2014*.Liptovský Mikuláš : Akadémia ozbrojených síl. 2014. ISBN 978-8040-495-6

HOFREITER, L. 2015. Internal factors of national security. In: *Security indicators in social environment*. Warszaw: Jagellonian institute , 2015.pp.7-17

HOFREITER,L. - ZVAKOVÁ, Z. *Teória bezpečnosti*. KRAKÓW: Wydawnictwo European Association for Security, 2019, ISBN 978-83-61645-35-1

HOFREITER, L. - KUBÍKOVÁ, Z. 2020. Theoretical basis of soft target protection In: Hofreiter, L. et al.: *Soft target protection : theoretical basis and practical measures*. Dordrecht: Springer Nature, 2020. ISBN 978-94-024-1757-9. - s. 149-160

HOLMQVIST, G.2012. *Inequality and Identity. Causes of War* ? Uppsala : Nordiska Afrikainstitutet, 2012. ISBN 978-91-7106-714-2

HOMER–DIXON, T. 2006. *The Upside of Down.* [online]. Dostupné na Internete: http://www.theupsideofdown.com/theargument.htm

HUMAN DEVELOPMENT REPORT 1994. *New Dimensions of Human Security.* [online] Dostupné na Internete: https://hdr.undp.org/system/files/documents//hdr1994encompletenostatspdf.pdf

SOROKIN, P. 2009. *Ruchliwość społeczna*. Warszawa: Wydawnictwo Instytutu filozofii i socjologii PAN. 2009. 540 s.ISBN 978-83-7683-002-5.

UNDP Special report. 2022. *New threats to human security in the Anthropocene:Demanding greater solidarity*. [online] Dostupné na Internete: https://hs.hdr.undp.org/pdf/srhs2022.pdf

prof. Ing. Ladislav HOFREITER, CSc.
Katedra bezpečnosti a obrany
Akadémia ozbrojených síl gen. M. Štefánika
Demänová 393, 031 01 Liptovský Mikuláš 1
e-mail: ladislav.hofreiter@aos.sk

PODPORA VOJENSKÉHO SPRAVODAJSTVA V PROSPECH OBLASTI BOJA PROTI IMPROVIZOVANÝM VÝBUŠNÝM PROSTRIEDKOM

MILITARY INTELLIGENCE SUPPORT IN FAVOUR TO THE AREA OF COUNTER IMPROVISED EXPLOSIVE DEVICE

Alexander HUGYÁR

ABSTRACT

Military Intelligence (MILINTEL) history is old as the warfare itself. With evolving trend of the Improvised Explosive Device (IED) attacks against coalition forces, the protection of the forces started to be more and more dependent on the information received before and during coalition forces deployment. Crucial information is provided by various MILINTEL elements, which contribution to countering IED attacks is narrated through this article's content. Moreover, this paper provides its reader with the cycle of MILINTEL activities that are inseparable part of the North Atlantic Treaty Organization's so called "Counter IED system".

Keywords: Military Intelligence, Improvised Explosive Device, Counter Improvised Explosive Device, Intelligence activities cycle, Military intelligence elements.

ÚVOD

História vojenského spravodajstva je od vekov neoddeliteľne spätá s vojenským umením. Už v biblických časoch Mojžiš vysielal svojich vyzvedačov aby sa zblížili a žili s obyvateľmi Kanaánu[1]. V tom období cieľom Mojžiša bolo naučenie sa zvyklostiam Kanaáncanov, odhalenie ich silných a slabých článkov spoločnosti. Postupne si Mojžiš týmto spôsobom vybudoval svoju armádu, ale aj bol schopný prevahy nad Kanaáncanmi.

V minulosti vojenské spravodajstvo a jeho služby boli využívané predovšetkým v čase vojny. Príkladom výsledku zlyhania a neuceleného systému vojenského spravodajstva v histórii Spojených štátov amerických počas druhej svetovej vojny je zničenie Pacifickej flotily pri útoku na Pearl Harbour (Watson, 2012).

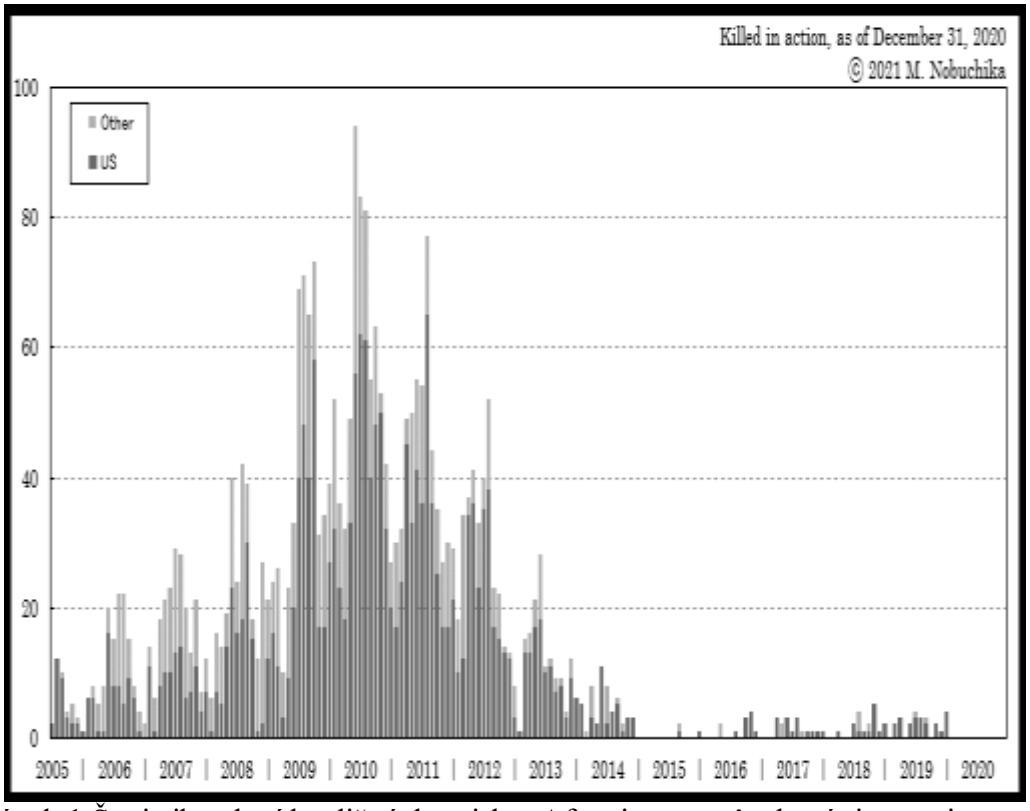
Rozmach vojenského spravodajstva v 20. storočí s analýzou informácii nastal v priebehu vojny v Iraku (1990 - 2003) a v Afganistane (2001 - 2021). V priebehu nasadenia koaličných síl Severoatlantickej aliancie (angl. *„North Atlantic Treaty Organization"*, skr. *NATO*) dochádzalo v prvých rokoch k značným stratám na životoch vojakov koalície, ale aj spriatelených - domácich bezpečnostných zložiek. Príčinou týchto strát bol nedostatok informácii o spôsobe boja protivníka.

Jedným zo zbraní, ktoré spôsobovali tieto straty boli použité improvizované výbušné prostriedky (angl. *„Improvised Explosive Device",* skr. *IED*), ktoré boli používané teroristami

[1] Kanaán, označenie územia predného východu, v súčasnosti odpovedá územiu Palestíny, https://www.britannica.com/search?query=Canaan

za účelom zmarenia plnenia úloh koaličných vojsk v ich úsilí budovania bezpečnosti v priestore nasadenia a s tým súvisiacou podporou vláde vo forme stabilizácie spoločnosti.

Postupným spoznávaním techník, taktík a procedúr (angl. *„Technics Tactics and Procedures“,* skr. *TTP*) protivníka, za pomoci vojenského spravodajstva a s tým následným zdokonaľovaním vojenských spôsobilostí dochádzalo k úspešnému boju proti útokom IED, ktorých výsledok je badateľný prostredníctvom poklesu obetí IED útokov z radu príslušníkov koaličných vojsk (viď. Obrázok 1).



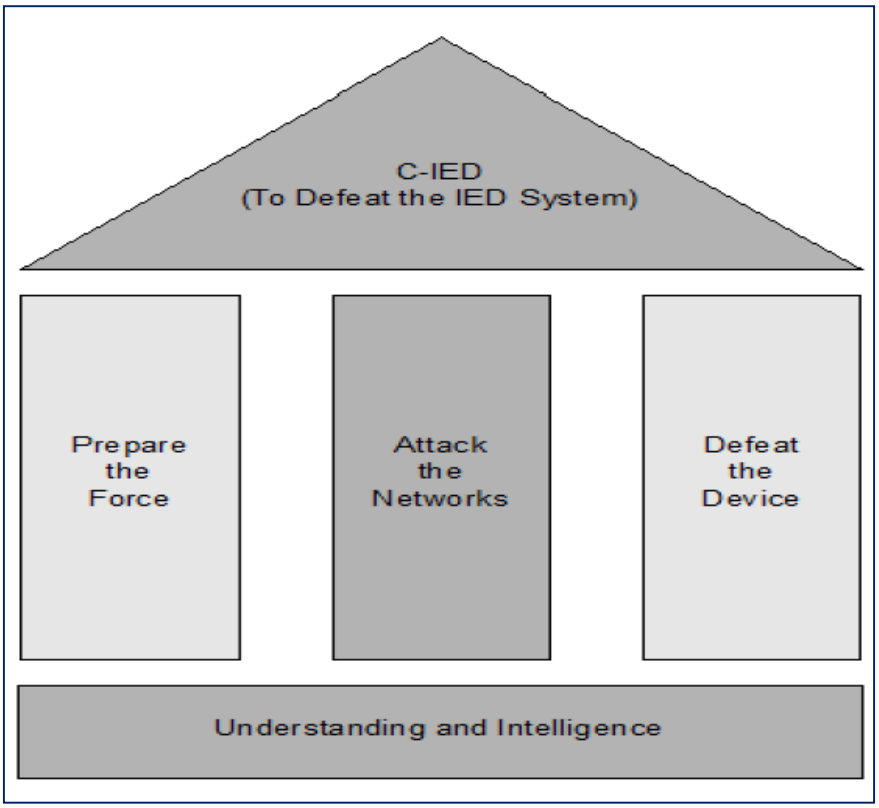
Obrázok 1 Štatistika obetí koaličných vojsk v Afganistane spôsobený improvizovanými výbušnými prostriedkami, roky 2005-2019
Zdroj: Nobuchika M., 2020

Úspešný boj proti IED a tým ochrana životov v priestore nasadenia koaličných síl neoddeliteľne súvisí s prepojením jednotlivých zložiek spravodajstva (angl. „*Inteligence Networking”*), ktorých činnosť je témou tohto príspevku.

1 POROZUMENIE VOJENSKÉHO SPRAVODAJSTVA PROSTREDNÍCTVOM PILIEROV C-IED

Severoatlantická aliancia (angl. *„North Atlantic Treaty Organization“*, skr. *NATO*) definuje vojenské spravodajstvo ako štruktúru pozostávajúcu z celkovej organizácie a hierarchie, procesov a systémov, v rámci ktorých vojenská spravodajská štruktúra NATO pôsobí a spolupracuje s inými národnými a medzinárodnými agentúrami a organizáciami s cieľom podporiť rozhodovanie funkcionárov s rozhodovacou právomocou na všetkých stupňoch riadenia (SOŠ, 2021, s. 352).

Koncepcia boja proti IED (angl. „*Counter Improvised Explosive Devices*“, skr. *C-IED*) v NATO je principiálne postavená na troch pilieroch, ktorých základ tvorí porozumenie spravodajstva (viď. Obrázok 2).



Obrázok 2 Prístup NATO k C-IED
Zdroj: AJP 3.15(C), p.24

Pilier prípravy síl je aplikovateľným pilierom opatrení pre všetky komponenty spoločných nasadených jednotiek. Pilier prípravy síl vyžaduje porozumenie operačného priestoru nasadenia koaličných síl. Z dôvodu efektívneho nasadenia spôsobilostí v boji proti IED útokom rozhodujúcu úlohu bude zohrávať štruktúra nasadených koaličných síl, ktoré musia byť primerane vycvičené, vyzbrojené a stmelené v súlade s ich plnením taktických úloh. Vycvičenosť, výzbroj a stmelenie koaličných síl bude odzrkadľovať proces spravodajských informácii, analýza získaných poznatkov a najlepších praktík (angl. *„Best Practices“*) s cieľom vytvoriť účinné TTP nasadených síl.

Prostredníctvom tohto piliera velitelia koaličných síl s ich vytýčenou právomocou zohrávajú kľúčovú úlohu pri implementácii a aktualizácii nových informácii, ktoré boli získané a následne analyzované spravodajskou činnosťou z bojiska. Medzi informácie, ktoré vojenské spravodajstvo zhromažďuje k podpore zlepšenia prípravy koaličných síl patrí pozorovanie miestneho obyvateľstva, odhaľovanie miest častých IED útokov, nezvyčajné – necharakteristické javy prostredia, označovanie miest IED útokov ich aktérmi, spôsob umiestnenia IED a pod. Všetky tieto informácie ovplyvňujú prípravu a výcvik príslušníkov koaličných síl, čím napĺňajú hlavné poslanie výcviku *„Cvič, ako bojuješ“* (angl. *„Train as you fight“*).

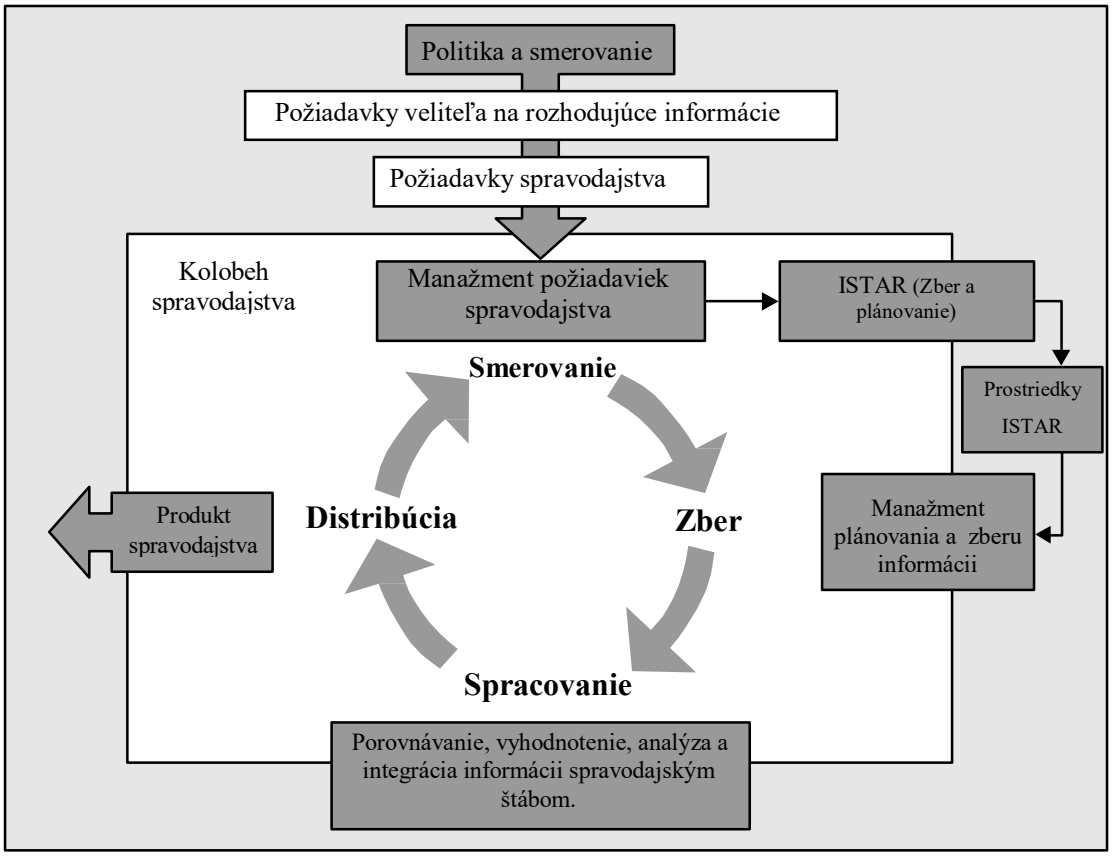
Pilier útoku proti sieťam je principiálnym pilierom v boji proti IED. V spoločnom priestore nasadenia bude tento pilier značne závislý na zdieľaní a poskytovaní informácii v mnohonárodnostnej štruktúre koaličných jednotiek. Tento pilier je charakteristický prevažne proaktívnou činnosťou, ktorá je riadená cestou spravodajských služieb. Cieľom

tejto činnosti je útok na slabé, zraniteľné články IED systému ako je eliminácia zdrojov a zásob komponentov IED, zmrazenie finančných zdrojov, identifikácia a neutralizácia lídrov teroristických buniek, zamedzenie regrutácie opozičných síl ako i izolácia teroristických skupín od miestneho obyvateľstva. Všetka táto činnosť, ktorá je vykonávaná spravodajskými službami je podmienená dostatočnou mierou exploatácie, ktorá je vitálnym komponentom spomínaných činností. Exploatácia svojim analytickým prístupom prispieva k odhaleniu zámeru útokov IED, objasneniu vzťahov medzi kľúčovými aktérmi a teroristickými bunkami ako i taktickým a technickým charakterom skonštruovaného prostriedku. Výsledkom exploatácie je prevencia ako i predvídanie pripravovaného IED útoku.

Pilier porazenia prostriedkov IED je proaktívnym a reaktívnym pilierom čoho výslednom je detekcia, neutralizácia prostriedku IED ako i konečné zníženie účinkov IED prostriedku. Hlavným cieľom piliera porazenia IED je udržanie a obnovenie schopnosti manévra vlastných síl a prostriedkov (AJP-3.12, s. 24). Merateľným ukazovateľom tohto piliera je záchrana životov vlastných síl, lokálneho obyvateľstva ale i materiálnych a hospodárskych hodnôt v priestore nasadenia. Výkonným prvkom tohto piliera sú plne vycvičené a bojaschopné EOD tímy so spôsobilosťou odstraňovať prostriedky IED. Okrem odstraňovania prostriedkov IED sa nasadené IED tímy podieľajú svojimi spôsobilosťami na technickej exploatácii, ktorá v konečnej miere rozvíja odhalenie používaných techník, taktík a procedúr teroristických skupín a tým podporuje činnosť spravodajských služieb (AJP-3.15, s. 53-67).

2 KOLOBEH SPRAVODAJSKÝCH ČINNOSTÍ PRISPIEVAJÚCICH K C-IED

Napĺňanie cieľov jednotlivých pilierov C-IED odzrkadľuje súhrn spravodajských procesov, ktorých kolobeh je zobrazený na Obrázku 3. Smerovanie vojenského spravodajstva určuje spresnenie rozhodujúcich požiadaviek operačného veliteľa (angl. „*Commander's Critical Requirements",* skr. *CCRs*), alebo stanovenie požiadaviek k priorite informácii (angl. „*Priority Information Requirements",* skr. *PIRs)*. Následne vojenské spravodajstvo, po obdržaní CCRs, alebo PIRs zhodnotí a prerozdelí veliteľove požiadavky do formy spravodajských požiadaviek (angl. „*Intelligence Requirements",* skr. *IRs)*.



Obrázok 3 Kolobeh spravodajských činností
Zdroj: Vlastné spracovanie podľa AJP 3.15 (A), p.52

Zber informácii je činnosť, ktorým spravodajské služby získavajú informácie k naplneniu stanovených IRs. Zber informácii zahŕňa plánovanie, koordináciu, a nasadenie prostriedkov spravodajstva, sledovania, zisťovania cieľov a prieskumu (angl. *"Intelligence, Surveillance, Target Acquisition and Reconnaissance"*, skr. *ISTAR*) a iných prvkov spravodajstva. ISTAR prispievajú k zberu, interpretácii, vyhodnoteniu a exploatácii informácii v organizačnej štruktúre nasadených síl. Informácie, ktoré boli zhromaždené podľa IRs sa následne spracujú podľa CCRs.

Činnosť spracovania informácií súvisí s porovnávaním, vyhodnocovaním, zlučovaním a objasňovaním informácii s ich interpretáciou k ďalšej distribúcii. Spracovanie informácii je spravidla úlohou operačnej spravodajsko - podpornej skupiny (angl. *„Operational Intelligence Support Group"*, skr. *OISG*), ktorá spolupracuje s národnými spravodajskými agentúrami. Následne OISG zabezpečuje v mieste pôsobenia zhrnutie informácii vo forme produktov v rámci všetkých spravodajských zdrojov (angl. *„All-Source Intelligence Products"*, skr. *ASIP*).

Distribúcia v kolobehu spravodajských činností predstavuje podávanie, rozosielanie spravodajských informácii v danom čase, stanovenej forme pre ich adresáta. V ďalšom rade je dôležité takto spracovaným informáciám priradiť príslušnú bezpečnosť – stupeň utajenia vzhľadom na ich dôležitosť pre určeného adresáta. Distribúcia informácii je vecou tzv. princípu *„Need to Know"* (AJP-3.15 (C), p. 43-44)

3 PRVKY SPRAVODAJSTVA PLNIACE ÚLOHY V PROSPECH C-IED

Kolobeh smerovania, zberu, spracovania a distribúcie informácii zabezpečujú v prospech C-IED prvky vojenského spravodajstva.

K týmto prvkom predovšetkým radíme:

- spravodajstvo, sledovanie, a prieskum (angl. „*Intelligence, Surveillance and Reconnaissance“,* skr. *ISR*),
- spravodajstvo ľudských zdrojov (angl. *„Human Intelligence“,* skr. *HUMINT*),
- spravodajstvo interpretácie získanej obrazovej dokumentácie (angl. „*Imagery Intelligence“,* skr. *IMINT*),
- spravodajstvo prostriedkov komunikácie (angl. „*Signals Intelligence“,* skr. *SIGINT).,*
- exploatácia materiálových a ľudských zdrojov (angl. „*Materiel and Personnel Exploitation“,* skr. *MPE*).

ISR predstavuje koordinovaný a integrovaný zber informácii, ich následné spracovanie a poskytovanie v požadovanom čase, s overeným stupňom dôveryhodnosti, s overenými súvislosťami ich detailov slúžiaci k zabezpečeniu činnosti veliteľov. V tejto súvislosti ISR sústreďuje svoje prostriedky na všetkých komponentoch síl pozemných, vzdušných a námorných na rôznych vrstvách toku informácii, ktoré sú získavané prostredníctvom senzorov. Výsledkom masového rozmiestnenia prostriedkov ISR na platformách komponentov je overenie dôveryhodnosti informácii po ich analýze.

HUMINT je prvkom spravodajstva, ktorý získava informácie prostredníctvom ľudských zdrojov. Informácie od miestneho obyvateľstva a bezpečnostných služieb hostiteľskej krajiny môžu v kolobehu informácii zreteľne prispievať k odhaleniu podozrivej činnosti v spoločnosti, ktoré by v danom priestore nasadenia mohli z dôvodu kultúrnych rozdielov, alebo miestnych pomerov inak koaličným silám uniknúť. HUMINT je jedným z hlavných zdrojov informácii v boji proti IED, ktorý identifikuje väzby jednotlivých aktérov v systéme prípravy a realizácie IED.

IMINT za pomoci nasadených senzorov umiestnených na platformách komponentov síl identifikuje a analyzuje napr. pohyb podozrivých osôb v ohniskách útokov (angl. *„Hot Spots“*), porušenie terénu s možným umiestnením IED. Následne IMINT prispieva k identifikácii a paralyzácii cieľov (angl. *„Targeting“*).

Stredom záujmu **SIGINT** sú komunikačné systémy a elektronické prostriedky. V procese C-IED, prvok spravodajstva SIGINT odhaľuje komunikáciu jednotlivých aktérov v systéme prípravy a realizácie IED za pomoci napr. odpočúvania ich rozhovorov, získavania dát z elektronickej pošty, prehľadu kmitočtov – kanálov rádiovej prevádzky a pod., čím je možné odhaliť úmysel a vzájomné prepojenie aktérov v ich hierarchii.

MPE je definovaný ako systematický zber a spravovanie informácii a ich distribúcia prostredníctvom spravodajstva, ktorý je výsledkom taktického vypočúvania, vyšetrovania a extrakcie dát z rekonštruovaných- obnovených zdrojov. MPE maximalizuje úsilie spravodajstva na vyhodnotenie dôkazového materiálu, ktorý prostredníctvom vhodne zvolených vedeckých metód a technológii prispieva k zadržaniu, usvedčeniu a konečnému odsúdeniu aktérov prípravy a realizácie IED útokov (No.09-49, p. 35-45).

MPE je tvorený nasledovnými disciplínami:

- analýzou zadržaných médií (angl. *„Seized media analysis“*),
- taktickým vypočúvaním a vyšetrovaním (angl. *„Tactical questioning“*),
- technickým spravodajstvom (angl. „*Technical Intelligence“*),

- spravodajstvom dôkazov a biometrických údajov (angl. „*Forensic and Biometric Intelligence*“).

Podporu prvkov spravodajstva, ktoré plnia úlohy v prospech C-IED je možné rozdeliť na dve etapy:

- pred nasadením do priestoru zodpovednosti,
- počas nasadenia v priestore zodpovednosti.

Vojenské spravodajstvo prostredníctvom svojich prvkov **pred nasadením** koaličných síl do operácií by mali poskytnúť jednotkám nasledujúce informácie o:

- historickom vývoji konfliktu v priestore nasadenia so všeobecnými informáciami o politickej, ekonomickej, právnej simulácii atď.,
- zvykoch obyvateľstva s hierarchiou uplatňovania miestnych autorít moci,
- používaných TTP protivníka s hlavnými druhmi ich výzbroje,
- systéme riadenia a velenia C-IED operácii a ich previazanie s činnosťou v prospech spravodajstva,
- identifikácii jednotiek protivníka a ich kľúčových aktérov, vodcov,
- konštrukcii používaných IED skonštruovaných protivníkom,
- jedinečnosti vplyvu terénu na nasadenie koaličných jednotiek s naučenými a aplikovateľnými TTP v danom priestore,
- systéme poskytovania spravodajských informácii v prospech EOD,
- obmedzeniach používania EOD výzbroje vplyvom činnosti protivníka.

Počas nasadenia v priestore zodpovednosti budú produkty spravodajstva poskytované vo forme spresnení pre danú oblasť – priestor zodpovednosti (angl. *„Area of Responsibility“*). Tieto informácie sa budú týkať nasledujúcich oblastí:

- rozsahu poskytovania spravodajských informácii v súlade s ustálenými operačnými postupmi,
- spresnenia a pravidelnej informácie o politickej, ekonomickej, právnej simulácii,
- spresnenia a pravidelnej informácie o hierarchii miestnych autorít moci,
- spresnenia procesu identifikácie cieľov (angl. *„Targetimg“*),
- spresnenia informácii o kredibilite miestnych agentúr spolupracujúcimi s koaličnými silami,
- spresnenia a pravidelnej informácie o zmenách v používaní TTP protivníka s hlavnými druhmi ich výzbroje,
- spresnenia a pravidelnej informácie o systéme riadenia a velenia EOD operácii a ich previazanie s činnosťou v prospech spravodajstva v súlade s ustálenými operačnými postupmi (SOP), zvlášť v čase preberania a odovzdávania úloh tzv. *“rotácie”*,
- spresnenia operujúcich jednotiek protivníka s ich kľúčových aktérmi,
- spresnenia miest so zvýšeným počtom IED útokov tzv. *„Hot Spots“*,
- spresnenia konštrukcie používaných IED,
- spresnenia obmedzenia používania výzbroje a výstroje vplyvom činnosti protivníka.

ZÁVER

V súčasnosti krajiny k získavaniu informácii okrem ľudských zdrojov využívajú k získavaniu informácii a k ich analýze množstvo moderných technológii. Satelity, ultraľahké lietadlá, elektronické systémy, kamery, zobrazovacie prostriedky a ich vzájomné prepojenie

ponúka obrovské možnosti ako získavať informácie v rozsahu, ktorý si človek v minulosti nebol schopný predstaviť.

Porozumenie, interpretácia a pochopenie získaných informácii, sociálnych, historických, antropologických, ekonomických a lokálnych podmienok v mieste pôsobenia operácie prispievajú v C-IED systéme k ochrane síl (angl. *„Force Protection"*, skr. *FP*), (AJP-3.14, s. 56).

Úspešný boj proti IED útokom vyžaduje fúziu a syntézu informácii zo všetkých zdrojov informácii. Prostredníctvom kolobehu spravodajských činností spravodajské služby podporujú činnosti nasadených koaličných síl, ktoré v rámci pilierov C-IED tvoria účinný systém boja proti IED útokom.

Obzvlášť v priestore nasadenia koaličných síl v priestore asymetrického boja je rozhodujúce prepojenie medzinárodných a mnohonárodnostných spravodajských kanálov so zdrojmi lokálnych - miestnych spravodajských informácii, ktoré budú využívať otvorené zdroje. K analýze týchto zdrojov informácii, ako i k ich poskytovaniu bude potrebné aby velitelia koaličných jednotiek s miestnymi orgánmi vopred dohodli podmienky manažmentu podľa ktorých sa tieto informácie budú zdieľať.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

AJP 3.12 Allied Joint doctrine for Military Engineering Edition C Version 1, Brussels: NSO, 2021.

AJP-3.14 Allied Joint Doctrine For Force Protection Edition C Version 1 Brussels: NSO, 2019.

AJP-3.15 Allied Joint Doctrine For Force Protection Edition A Version 1 Brussels: NSO, 2015.

AJP-3.15 Allied Joint Doctrine For Countering Improvised Explosive Devices Edition C Version Brussels: NSO, 2018.

Britannica, The Editors of Encyclopaedia, 2019. Canaan. In *Encyclopedia Britannica*, [online]. 11.10.2019 [cit. 29.08.2022] Dostupné na internete: https://www.britannica.com/search?query=Canaan.

Elektronický lexikón slovenského jazyka, 1987, [online] 1987 [cit. 29.08.2022] Dostupné na internete: http://www.slex.sk.

MICHAUD, Y. The silver bullet: The comprehensive approach to Counter Improvised Explosive Devices, 2013. In *JCSP 39 Master of Defence Studies* [online]. 2013 [cit. 29.08.2022] Dostupné na internete: https://www.cfc.forces.gc.ca/259/290/299/286/michaud_y.pdf.

NATO ACT. Commanders' and Staff Handbook for Countering Improvised Explosive Devices, SHAPE, TSX 0170/TT-7579/Ser: NU0462, Headquarters, Supreme Allied Commander Transformation, NATO SACT Norfolk, USA, 2011.

NATO. AJP-3.15 Allied Joint Doctrine For Countering Improvised Explosive Devices Edition C Version. Brussels: NSO, 1 February 2018.

No.09-49 IED Defeat Ledear's Handbook; Tactics, Technics and Procedures, Center for Army Lessons Learned, 2009, p. 39-45.

NOBUCHIKA, M. 2020 Coalition Military Deaths in Afghanistan War In: *War in terror* [online]. 31.01.2020 [cit. 29.08.2022], Dostupné na internete: https://web.econ.keio.ac.jp/staff/nobu/iraq/en/casualties.html.

PORADA, V. A kol. 2019. Bezpečnostní vědy. Plzeň: vydavatelstvý a nakladatelstvý Aleš Čenek s.r.o., 2019, s. 80-83 ISBN 978-80-7380-758-0.

SOŠ 3680 AAP-6 Slovník termínov a definícií NATO (vydanie 12), Bratislava, December 2021

WATSON, B.W. 2012. Intelligence. In *Encyclopedia Britannica*, [online]. 29.02.2012 [cit. 29.08.2022], Dostupné na internete: https://www.britannica.com/topic/intelligence-military.

pplk. Ing. Alexander HUGYAR, externý doktorand Katedry bezpečnosti a obrany
Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 01 Liptovský Mikuláš, SR
alexander.hugyar@eodcoe.org

PRÍSTUP SEVEROATLANTICKEJ ALIANCIE K FENOMÉNU ÚTOKOV VYKONÁVANÝCH PROSTREDNÍCTVOM IMPROVIZOVANÝCH VÝBUŠNÝCH PROSTRIEDKOV

THE NORTH ATLANTIC THREATY ORGANIZATION APPROACH TO IMPROVISED EXPLOSIVE DISPOSAL ATTACKS PHENOMENA

Alexander HUGYÁR

ABSTRACT

Improvised Explosive Device (IED) attacks are one of the global threats that have been frequently resonating across the security environment as one of the significant threats for years. Empowered by access to information and countless reports that media brings in a form of statistics to public on daily basis (mass causalities, injured victims, damaged infrastructure) there are affecting the human feeling of security at all.

Bearing in mind the IED attacks‘ implications on security, this article develops the IED phenomena from the North Atlantic Treaty Organization (NATO) perspective. As one of the principles for NATO’s policy in countering IED threat, the article subjects to NATO’s achievement on common understanding of the IED threat, IED attack event chain and the IED’s functional areas.

Keywords: Security, Improvised Explosive Device (IED), IED attack, IED event chain, IED actor.

ÚVOD

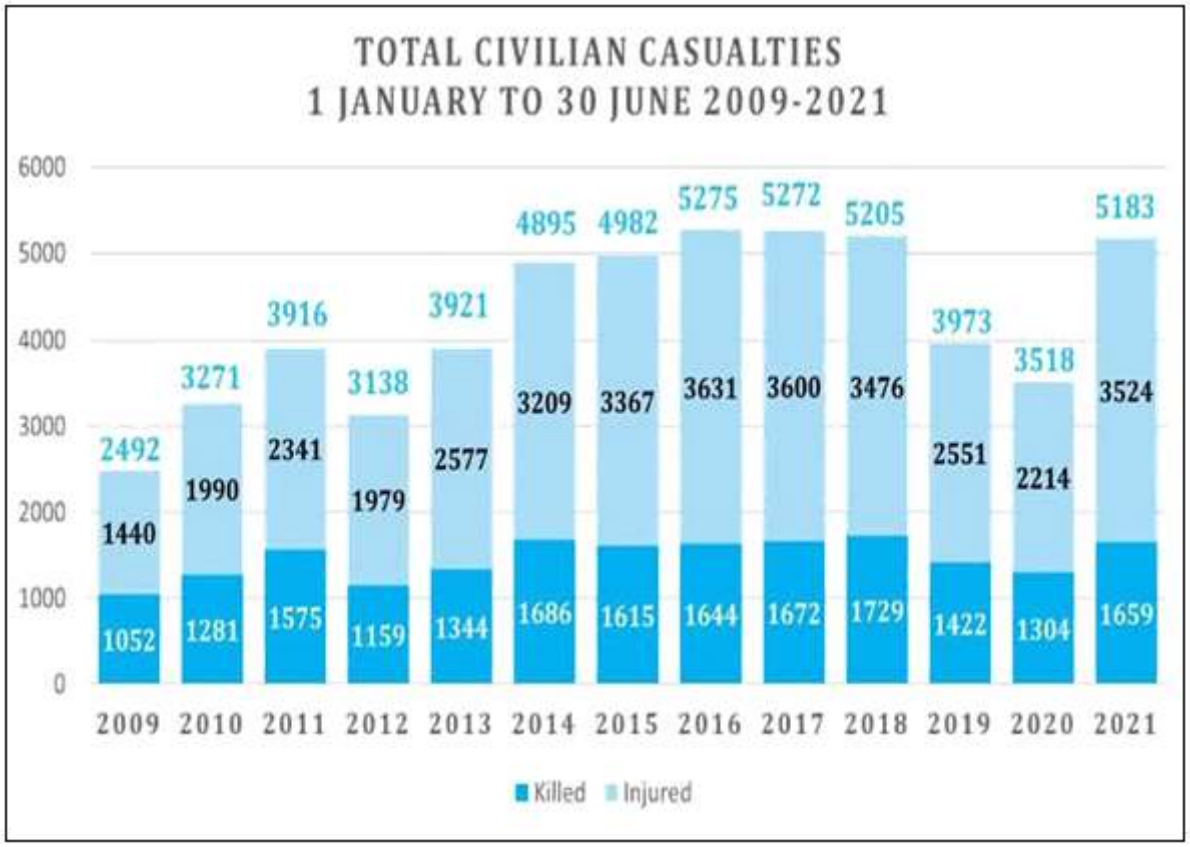
Útoky vykonané prostredníctvom improvizovaných výbušných prostriedkov majú pomerne dlhodobú a bohatú históriu. Medzi prvé útoky vykonané prostredníctvom improvizovaných výbušných prostriedkov, ktoré boli zaznamenané vo Veľkej Británii, patrí zavraždenie Jakuba I, Stuartského v roku 1605. Spomínaný útok vykonal Guy Fawkes, ktorého motívom bol pokus o zvrhnutie parlamentu Británie (DHS, C IED SP, s. 2).

Postupný rozvoj zbraní a munície v Napoleonskom Francúzsku (1769-1821), spojený s ich dostupnosťou, napomohol sérii útokov s využitím improvizovaných výbušných prostriedkov proti Napoleonovi a jeho stúpencom. Konkrétne, 24. decembra 1800 bol vykonaný útok na Napoleona, ktorý sa so svojim sprievodom presúval v Paríži. Nakoľko útočníci zle načasovali iniciáciu improvizovaného výbušného prostriedku, Napoleon sa účinkom útoku vyhol. Avšak, výsledky incidentu potvrdili účinnosť prostriedku, ktorý usmrtil v uliciach Paríža 22 príslušníkov Napoleonovej družiny a zranil desiatky obyvateľov.

Časté použitie útokov prostredníctvom improvizovaných výbušných prostriedkov bolo neskôr pozorované počas občianskej vojny Spojených štátoch amerických v rokoch 1861-1865 na území Mobile Bay a Petersburgu a počas tzv. *„Arabských vzbúr“* v rokoch 1916-1918 (Murphy, 2011, s.52). V týchto obdobiach bolo hlavným motívom útokov maximalizovať obavy protivníka prostredníctvom momentu prekvapenia spojené so stratami jeho bojového potenciálu. Podobne útoky prostredníctvom improvizovaných výbušných prostriedkov boli monitorované v každom prebiehajúcom konflikte počas 20 storočia. Medzi tieto konflikty radíme 2. svetovú vojnu (1939-1945), vojnu vo Vietname (1954-1975), konflikt na území Severného Írska (1968-1998), vojnu v Iraku (1990-2003), vojnu v Afganistane (1979-1989 a 2001-2021) a pod.

Severoatlantická aliancia (v ďalšom texte NATO) pod pojmom improvizované výbušný prostriedok (angl. *„Improvised Explosive Device“,* skr. *IED*) rozumie prostriedky umiestnené, alebo vyrobené improvizovaným spôsobom, zahrňujúce ničivé, smrteľné, škodlivé, žiarové alebo zápalné chemické látky, navrhnuté na ničenie, zmrzačenie, odpútanie alebo rušenie (SOŠ, s. 338). Tieto prostriedky môžu obsahovať súčasti z vojenských zásob, ale zvyčajne sú vyrobené z nevojenského materiálu. Do tejto kategórie sú zahrnuté i nástražné výbušné systémy (angl. „*Booby trap“*), ktoré sú definované ako prostriedok vytvorený, zostavený, alebo prispôsobený na zabitie alebo zranenie, ktoré sa uvedie do činnosti, ak osoba naruší zdanlivo neškodný predmet, alebo sa k nemu priblíži, alebo pri zdanlivo bezpečnej manipulácii ho privedie k činnosti (SOŠ, s. 118).

Súčasné, operujúce teroristické skupiny realizujú útoky IED na taktickej úrovni, avšak s ohľadom na veľký počet obetí majú tieto útoky v bezpečnostnom prostredí Severoatlantickej aliancie strategické následky. Príkladom sú stále trvajúce nepokoje v Afganistane. Podľa dostupnej štatistiky, spracovanej Organizáciou spojených národov (viď. Obrázok 1), počet obetí nevybuchnutých výbušných prostriedkov aj po ukončení misie krajín Severoatlantickej aliancie má v Afganistane rastúcu tendenciu.



Obrázok 1 Štatistika obetí nebezpečných účinkov nevybuchnutých výbušných prostriedkov za rok 2009-2021

Zdroj: https://unama.unmissions.org/civilian-casualties-set-hit-unprecedented-highs-2021-unless-urgent-action-stem-violence-%E2%80%93-un-report

Z tohto celkového počtu obetí, predstavujú obete IED útokov až 38 percent (UNAMA, Civilian causualities, 2021). Berúc do úvahy narastajúci trend IED útokov v globálnom

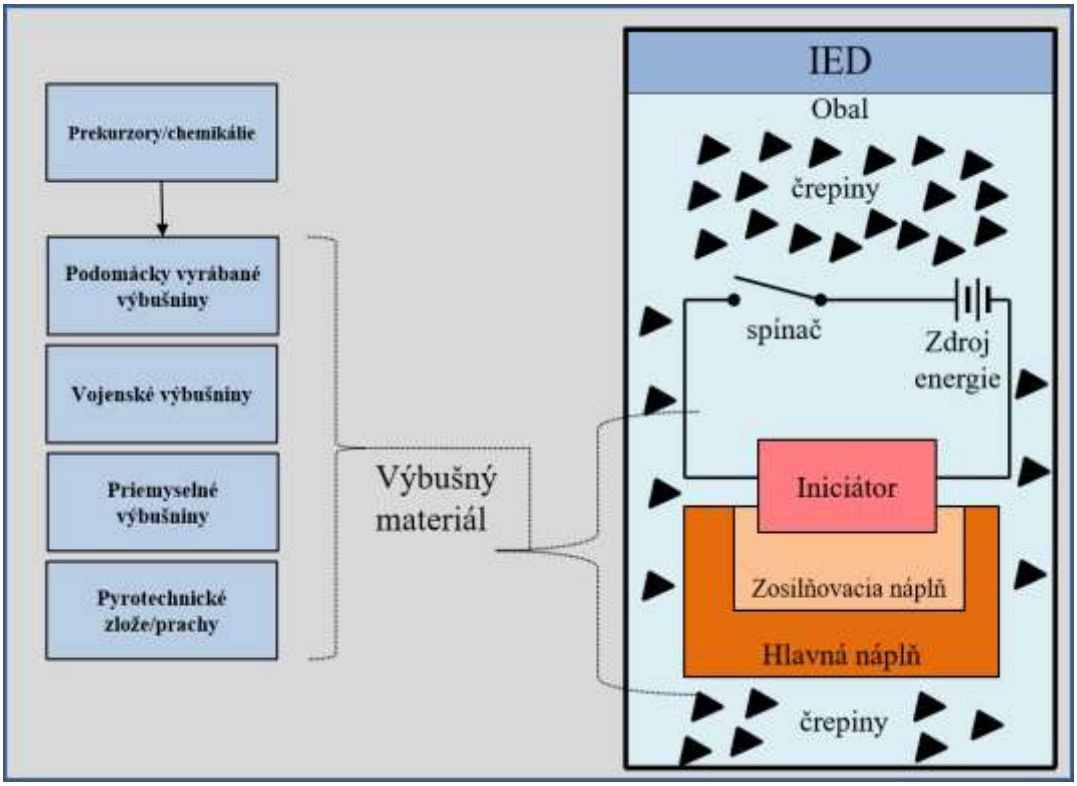
bezpečnostnom priestore, je cieľom tohto príspevku poukázať na základné pojmy a funkčné činnosti, ktoré súvisia s fenoménom IED v kontexte Severoatlantickej aliancie.

1 ZÁKLADNÉ ZLOŽENIE A ROZDELENIE IED

Vo vojenskej terminológii NATO sa IED delia do druhov podľa využívania rôznych technológií a druhu použitých materiálov. Každé IED (viď Obrázok 2), bez rozdielu požitia technológii je zložené z nasledujúcich častí:

- hlavnej náplne,
- iniciátora,
- spínača,
- zdroja energie.

Výbušný reťazec IED, ktorý je tvorený výbušným materiálom, môže okrem hlavnej náplne a iniciátora obsahovať aj zosilňovaciu náplň, ktorá plní úlohu prenosu výbušnej reakcie z iniciátora na hlavnú náplň. Pôvod výbušnín v spojitosti s IED je závislý na ich dostupnosti s využitím vojenských, priemyselných, ale aj bežných prekurzorov a chemikálii. Práve dostupnosť komerčného materiálu akými sú v podstate neškodné prekurzory a chemikálie, sa dajú vyrobiť za pomoci zvolených chemicko - technologických postupov a ich kombinácie tzv. podomácky vyrábané výbušniny.



Obrázok 2 Konštrukcia IED s jednotlivými komponentami IED
Zdroj: Vlastné spracovanie podľa Hotchkiss P., SAND2018-0766B Explosive Threats – The Challenges They Present and Approaches to Countering Them, 2018, Figure 2

Hlavná náplň IED nemusí vždy predstavovať iba výbušný materiál. K zvýšeniu ničivého účinku IED sa môžu využiť aj materiály nukleárneho, biologického, alebo chemického charakteru. Obal IED môže z dôvodu jeho maskovania pripomínať predmety bežného - denného použitia (krabice, termosky, vodovodné potrubie a pod.), resp. v prípade

zapustenia IED môže byť ako obal využitá pôda, stena, vozidlo, bicykel, ale aj rôzne torzá ľudských tiel a živočíchov.

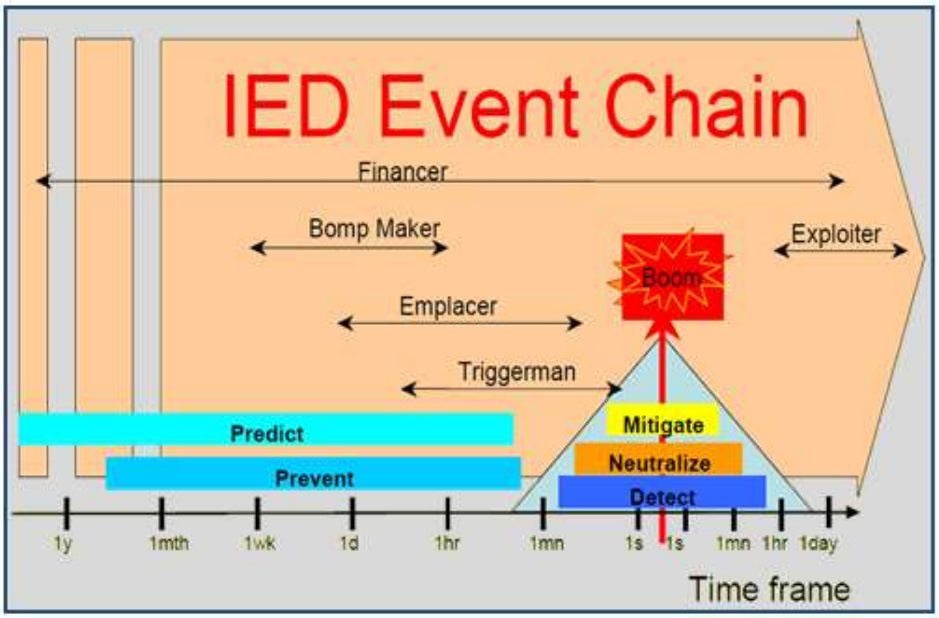
NATO rozdeľuje IED z dvoch pohľadov. Prvým pohľadom je z hľadiska technickej kategorizácie. Technická kategorizácia zahŕňa hierarchický konštrukčný postup vyhotovenia IED a jeho jednotlivých prvkov (viď. Obrázok 2). Komponenty identifikované technickou kategorizáciou sú vlastne po výbuchové elementy, z ktorých sa prostredníctvom ich analýzy zrekonštruuje IED. Druhý pohľad rozdelenia IED podľa taktickej charakteristiky, sa snaží objasniť akým spôsobom bol útok IED vykonaný, alebo naplánovaný k jeho konečnej realizácii. Táto oblasť sa sústreďuje predovšetkým na spôsob použitia IED, resp. snaží sa odhaliť úmysel použitia IED (ATP-3.12.1.1 (B), 2017, s. 13-15).

Obidva pohľady rozdelenia IED prispievajú k prevencii proti uskutočňovaniu útokov IED ako aj k objasňovaniu už vykonaných útokov IED a ich aktérov.

2 AKTÉRI IED ÚTOKOV

K základným predpokladom účinných opatrení proti IED patrí pochopenie prípravy a používania IED, s cieľom získania čo najhodnovernejších informácii o aktéroch zapojených do prípravy a realizácie útokov IED.

Všetky bunky IED útočníkov nie sú podobné, ale ich vykonanie smeruje k jednému organizačnému vzoru. Charakteristický vzor prípravy a realizácie IED útokov s ich aktérmi je zobrazený na Obrázku 3.



Obrázok 3 Systém prípravy a realizácie IED útokov
Zdroj: https://reliefweb.int/sites/reliefweb.int/files/resources/Explosive-Violence-Monitor-2020-V3-single-pages.pdf

Systém prípravy a realizácie IED útokov zahŕňa štyroch kľúčových aktérov, ktorí plnia rôzne úlohy. Popis aktérov IED útoku s ich určenými úlohami je uvedený v nasledujúcich bodoch:

a) Aktér zodpovedný za financovanie

Na vrchole tejto pyramídy je plánovač, alebo finančník (angl. „*Financier*“), ktorý je veľmi často vzdelaný a inteligentný človek, avšak ideologicky motivovaný

jedinec. Vo väčšine prípadov zabezpečuje v systéme prípravy a realizácie IED dostatočné zdroje k obstarávaniu materiálnych, ale i ľudských zdrojov a je hlavou, organizátorom IED útokov.

b) Aktér zodpovedný za konštrukciu IED

Zaujíma v systéme prípravy a realizácie IED útokov druhé najvýznamnejšie miesto v poradí. Je to zvyčajne ideologicky motivovaný jedinec, podobne zmýšľajúci a oddaný poslaniu, ktoré je diktované organizátorom IED útoku.

Technické zručnosti konštruktérov IED (angl. *„Bomb maker"*) v komunite postupom času narastajú tak, ako narastajú ich úspechy. V mnohých prípadoch, sú za účelom propagandy vedomosti o konštrukcii IED rozširované medzi teroristickými bunkami pomocou internetu. V súčasnosti je bežné, že konštruktér IED k zvýšeniu ničivej sily využíva usmernené nálože, alebo IED s črepinovým účinkom.

c) Aktér zodpovedný za umiestnenie IED

Ďalšou dôležitou osobou v systéme prípravy a realizácie IED útoku je osoba zodpovedná za umiestnenie IED (angl. *„Emplacer"*). Táto osoba má zvyčajne vojenský výcvik a je schopná nepozorovane preniknúť do prostredia, prepraviť, umiestniť a zamaskovať prostriedok IED.

Nepozorované premiestnenie IED z miesta konštrukčnej dielne a jeho umiestnenie pozdĺž frekventovanej cesty vyžaduje určitú dávku skúseností a odvahy. Osoba zodpovedná za umiestnenie IED vie, že ak bude odhalená pri umiestňovaný IED, môže byť zabitá. Z tohto dôvodu musí byť podrobne oboznámená s prostredím, v ktorom bude útok IED vykonaný, a zaistená pozorovateľom. Úlohou pozorovateľa je upozorniť aktéra na príchod napr. vojenskej, alebo policajnej hliadky.

Aktéra zodpovedného za umiestnenie IED je veľmi ťažké nahradiť spomedzi ostatných príslušníkov prípravy a realizácie IED útokov. V prípade jeho neutralizácie je činnosť teroristickej bunky aktérov IED aspoň dočasne prerušená, pokiaľ ju nenahradí niekto iný do momentu keď bude bunka opäť stmelená plniť jej protispoločenské poslanie.

d) Aktér zodpovedný za iniciáciu IED

Aktér zodpovedný za iniciáciu IED (angl. *„Triggerman"*) zodpovedná za iniciáciu - odpálenie IED. V prípade IED umiestnených vo vozidle (angl. *„Vehicle Borned IED",* skr. *VBIED)* tento jedinec odpáli IED za pomoci spínača, na diaľku napr. rádiom, alebo po drôte. Odpálenie diaľkovými prostriedkami je uprednostňované, pretože nevystaví aktérov IED útoku priamemu účinku výbuchu, znižuje možnosť ich odhalenia, ako aj zadržanie tohto aktéra IED útoku na mieste IED útoku.

3 FUNKČNÉ ČINNOSTI ZNIŽUJÚCE IED ÚTOKY

Z doterajších skúseností v oblasti boja proti IED útokom, k efektívnym prvkom opatrení k zamedzeniu IED útokov patria tzv. funkčné činnosti predvídavosť a prevencia.

Funkčné činnosti ako detekcia, neutralizácia a zmiernenie účinkov IED sú súčasťou opatrení až po potvrdenom výskyte IED. Detekcia, neutralizácia a zmiernenie účinkov súvisia s bezprostredným zásahom a následným odstraňovaním IED prostredníctvom odborne vycvičeného personálu.

a) Predvídavosť

Cieľom predvídania (angl. *„Prediction")* je identifikácia kritických bodov v organizácii prípravy IED ako i v konštrukcii samotných IED. Predvídanie je tesne spojené so spravodajskými schopnosťami NATO, zapojením technológií a mechanizmov k identifikácii a pochopeniu výzbroje a infraštruktúry protivníka napr. spôsobilosti technickej exploatácie[1]. Predvídavosť predstavuje sústreďovanie veľkého množstva informácií na základe ktorých sa identifikujú pravidlá a zvyky používané aktérmi IED útokov.

Následne po získaní informácii spravodajské služby prehodnocujú ciele protivníka, identifikujú oblasti aktivít IED útokov, označujú priestory, na ktoré musí byť zameraná zvýšená pozornosť (angl. *„Hot Spots"*), hľadajú sa kľúčové rysy taktík techník a procedúr (angl. *„Tactics Technics and Precedures*", skr. *TTP*) používaných protivníkom so zámerom predísť konečnému umiestneniu IED.

b) Prevencia

Hlavným cieľom prevencie (angl. *„Prevention"*) je eliminácia kritických bodov v organizácii prípravy IED i v konštrukcii samotných prostriedkov. Aktivity podporujúce prevenciu sú ofenzívne činnosti, ktoré sú plánované a riadené na všetkých úrovniach velenia a riadenia NATO, s cieľom eliminovať úmysel a schopnosti protivníka zostrojovať a používať IED. Aktivity funkčnej činnosti zahŕňajú velenie a riadenie, koordináciu spravodajskej činnosti, smerovanie toku informácií a hlavne odstraňovanie nevybuchnutej munície ako možného zdroja komponentov IED.

Preventívne opatrenia môžu byť vykonávané napr. na základe hlásenia podaného veliteľmi hliadok o podozrivom správaní obyvateľstva, alebo na základe potvrdenia nezvyčajných prvkov vedúcich k odhaleniu TTP protivníka. Preventívne opatrenia ovplyvňujú rozhodovací proces manévru operačných veliteľov NATO napr. stanovením presmerovania trasy presunu, stanoveniu optimálnej rýchlosti presunu, vzdialeností medzi vozidlami a pod. V neposlednom rade k ochrane vlastných síl, jednotky operujúce v takomto asymetrickom prostredí by mali byť primerane vyzbrojené prostriedkami odolnými proti výbuchu, ktoré sú špeciálne účelovo odolné proti rádovo vysokému stupňu ničivých účinkov výbuchu.

c) Detekcia

Detekcia IED (angl. *„Detection"*) obsahuje všetky činnosti, prostriedky a technológie (vrátane psov vycvičených na vyhľadávanie výbušných prostriedkov), smerujúce k lokalizácii aktérov IED útokov, detekcii a identifikácii IED prostriedku s jeho časťami, ako aj infraštruktúry kde sa IED prostriedky zhotovujú, poprípade uskladňujú.

Aktivity spojené s detekciou sú podmienené schopnosťou integrácie technológií, spravodajských informácií a výcvikových metód. Ich cieľom je zistiť miesto uloženia IED, tak rýchlo, ako je to v danej situácii možné, či už v priebehu zhotovovania IED, prepravy IED, alebo miesta umiestnenia IED. Vojenský personál, príslušníci vojenskej polície alebo ženisti, ktorí preverujú komunikácie, musia byť vycvičení a skúsení na to, aby dokázali odhaliť napr. samovražedného atentátnika pri

[1] Definícia pojmu *„Technická exploatácia* (angl. *„Technical Exploitation"*) je v terminologickom procese NATO termínov (https://nso.nato.int/nso/home/main/home, 15.2.2022). Je to systematický proces využívania technických a vedeckých metód k získaniu cenných informácii z materiálu exploatácie, ktorý bol zhromaždený z bojiska. Príkladom materiálu exploatácie radíme odtlačky prstov, stopy DNA, prostriedky digitálnych médií, dokumentáciu, ukoristené zbrane a pod.

bežnej nepravidelnej kontrole. Neoddeliteľnou - základnou súčasťou detekcie IED tvorí spravodajské vyhodnotenie bojiska, ktoré na základe sústreďovania informácií vykonáva analýzu trendov vývoja IED.

d) Neutralizácia

Táto funkčná činnosť predstavuje širokú škálu prípravných a výkonných opatrení a metodík na to, aby mohli byť IED a jeho komponenty rozrušené, zaistené proti nežiaducemu výbuchu, bezpečne zlikvidované alebo zničené. Neutralizácia (angl. *„Neutralization"*) nie je zameraná iba na zaistenie bezpečného prechodu okolo IED, ale aj na bezpečné odstraňovanie IED prostredníctvom spôsobilosti NATO odstraňovať nevybuchnuté výbušné prostriedky (angl. *„Explosive Ordnance Disposal"*, skr. *EOD*).

e) Zmiernenie účinkov

Zmierňovanie účinkov výbuchu IED (angl. *„Mitigation")* zahŕňa činnosti zamerané na znižovanie zraniteľnosti príslušníkov jednotiek NATO, najmä použitím technických riešení a štandardizáciou výcviku a vzdelávania. Jedným zo spôsobov zmierňovania účinkov je zvyšovanie individuálnej bezpečnosti prostredníctvom nových typov prostriedkov individuálnej ochrany, nových typov panciera, nových metód výcviku, ktoré eliminujú TTP protivníka. Zníženie útokov IED tiež predstavujú netradičné úlohy ako napríklad odstraňovanie odpadkov okolo ciest, v ktorých by sa mohli ukrývať IED a odťahovanie opustených vozidiel z toho istého dôvodu (ATP-3.12.1.1 (B), 2017, s. 13-15).

4 PRÍSTUP SEVEROATLANTICKEJ ALIANCIE V BOJI PROTI IED

Hlavným cieľom boja proti útokom IED patrí prevencia kritických bodov v organizácii, ktoré pripravujú IED útoky a tým zníženie možností konštrukcie samotných IED prostriedkov. V operáciách NATO sú aktivity podporujúce prevenciu ofenzívne činnosti, ktoré sú plánované a riadené na všetkých úrovniach velenia a riadenia. Tieto aktivity zahŕňajú koordináciu spravodajskej činnosti, tok informácií a hlavne odstraňovanie nevybuchnutej výbušných prostriedkov, ktorého princípmi sú funkčné činnosti uvedené v časti 3 tohto príspevku.

V januári 2010 agentúra NATO pre velenie a riadenie a komunikáciu (angl. *„NATO Command, Control and Communication Agency"* , skr. *NC3A*) vypracovala akčný plán boja proti improvizovaným výbušným prostriedkom (angl. *„C-IED Action Plan"*). Akčný plán C-IED identifikuje nedostatky v oblasti boja proti IED s ich finančnou implikáciou a následnou implementáciou, k dosiahnutiu maximálnej ochrany príslušníkov nasadených síl, ale aj obyvateľstva kde bola zaznamenaná, alebo sa potvrdila hrozba IED.

K zvýšeniu spoločnej spôsobilosti v boji proti IED boli identifikované organizačné zložky NATO a ich úlohy nasledovne:

- NC3A je centrálnym koordinátorom všetkých úloh. V súlade s konkrétnou úlohou akčného plánu NC3A zodpovedá za vykonávanie výskumu, rozvoj technológii, kybernetickú obranu a obstarávanie vybavenia C-IED. Koordinácia plnenia úloh NC3A sa vykonáva prostredníctvom aktívnej účasti na konferencii národných riaditeľov pre vyzbrojovanie členských krajín NATO (angl. *„National Armament Directors Conference"*, skr. *CNAD*). K previazanosti úloh vyplývajúcich z akčného plánu prispieva tzv. Program práce v oblasti boja proti terorizmu (angl. *„Defence Against Terorrism Program of Work"*, skr. *DAT POW*), ktorý pojednáva o nových technológiách a ich testovaní. Výsledkom DAT POW sú nové technológie a metódy

v oblasti detekcie, zníženia účinkov asymetrickej hrozby IED, ktoré podporujú odhaľovanie agentov IED prostredníctvom zberu biometrických údajov, technickej exploatácie a konečného odstraňovania IED z miesta lokalizácie prostriedku (NATO Web page, Coutering Terrorism, 2022).

- Organizačná zložka NATO pod anglickým názvom *„Emerging Security Challenges Division,* skr. *ESCD"* má za úlohu koordinovať expertov v oblasti bezpečnostných technológií zameraných na vývoj a využitie senzorov schopných detekcie a identifikácie výbušného materiálu. ESCD prostredníctvom vojenských organizácii, výskumných centier realizuje množstvo projektov. Jedným z inštitúcii, ktoré riadia riešenie projektov patria tzv. Centrá výnimočnosti NATO (angl. *„Centres of Excellence",* skr. *COEs*)[2].

Príkladom sú projekty Medzinárodného centra výnimočnosti v oblasti EOD (angl. *„Explosive Ordnance Centre of Excellence,* skr. *EOD COE"*), ktorého hosťujúcou krajinou je Slovenská republika. EOD COE od svojho vzniku (2011) riadi a podporuje projekty DAT POW. Medzi tieto projekty patrí séria podujatí *„EOD Demonstrations and Trials – EOD D&T"*, ktorého cieľom je spojiť inštitúcie z ozbrojených zložiek a zborov, akademickú obec a priemysel k identifikácii možných technologických riešení v oblasti EOD. Výsledkom jednej zo série EOD D&T je úspešne ukončený projekt s názvom *„Exoskeleton in the Battlefield"* (2017-2019). Hlavným výstupom tohto projektu je koncept NATO, ktorý spresňuje integráciu technológii uľahčujúcich činnosť príslušníkov NATO prostredníctvom využívania tzv. *„Exoskeleton for Human Performance Agmentation - EHPA"* (NATO EOD COE, EPHA).

Spomínaný príklad projektu DAT POW bol sponzorovaný priamo zo zdrojov ESCD. V súčasnosti EOD COE rozbieha podobne sponzorovaný projekt pod názvom *„EOD-IEDD Virtual Reality/Extended Reality – VR/XR Training and Combat Support Kit"* (2022-2026). Cieľom tohto projektu je skrátenie výcviku odborne spôsobilého personálu schopného odstraňovať nevybuchnuté výbušné prostriedky prostredníctvom virtuálnej a rozšírenej reality, vrátane výcviku IED (NATO EOD COE, EOD-IEDD VR-XR).

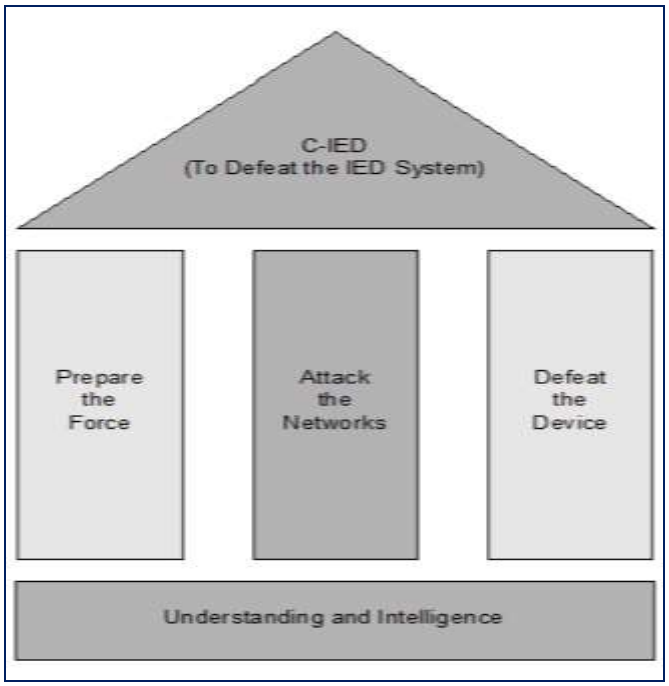
Rozsah zodpovednosti C-IED vychádza z doktríny NATO pre spoločné operácie (angl. *„Allied Joint Doctrine for the Conduct of Operations"*, ozn. AJP-3 (B)). NATO pod pojmom C-IED rozumie prístup operačných veliteľov s ich dostupnými prostriedkami čeliť hrozbe IED, a to prostredníctvom narušenia sietí aktérov IED útoku, prípravou koaličných síl kde bola zaznamenaná hrozba IED, ako aj znížením účinkov IED prostredníctvom k tomu určených špecialistov EOD (AJP-3, 2019, s.123-125). Tento prístup NATO je detailne rozpracovaný vo forme C-IED doktríny (angl. „ *Allied Joint Doctrine For Countering Improvised Explosive Devices*", skr. *C-IED doctrine*).

Celkový boj NATO proti IED je tvorený nasledujúcimi - podpornými piliermi:

- prípravy síl (angl. *„Prepare the Force"),*
- útoku na siete (angl. *„Attack the Network"*),
- porazenia prostriedkov IED (angl. *„Defeat the Device"*), (*AJP 3.15 (C), p.1-6).*

Základ účinnej podpory všetkých troch pilierov C-IED predstavuje pochopenie vojenského spravodajstva. Previazanie a funkčnosť C-IED pilierov je predpokladom k úspešnému boju proti IED (angl. *„Defeat the IED System"*). Vizuálne prístup NATO k C- IED je zobrazený na Obrázku 4.

[2] Zoznam akreditovaných EOD COE je aktualizovaný na stránke NATO Transformation Network.



Obrázok 4 Prístup NATO k C-IED
Zdroj: AJP 3.15 (C), p.1-6

ZÁVER

V súčasnom svete informovanosti a rýchlosti prenikania informácii prostredníctvom médií sú útoky IED s ich masovými - ničivými účinkami negatívne vnímané jedincom ako jedna zo závažných bezpečnostných hrozieb. Vnímané straty na životoch, zranenia obyvateľov v mieste útoku IED, zdemolované budovy a infraštruktúra oberajú človeka, ako člena spoločnosti, o všeobecný pocit bezpečnosti. Útoky IED majú niekoľko charakteristických aktérov, ktorí sa podieľajú na realizácii útokov IED. Okrem útokov IED namierených proti príslušníkom koaličných síl v mieste ich pôsobenia, sú obeťami týchto IED útokov aj civilné - nezainteresované osoby, čo z morálneho hľadiska konfliktu prináša daň vo forme straty nevinných životov.

Fenomén IED ako druh taktickej zbrane agresorov predstavuje svojim ničiacim potenciálom strategický dopad na bezpečnosť NATO (AJP-3.15, 2018, s. 25). Z pohľadu zabezpečenia boja proti IED má NATO spracovanú sériu štandardizačných dokumentov ako aj projekty, ktoré podporujú boj proti IED. Spoločne a jasne stanovené kompetencie, ktoré sú obsahom NATO publikácii na strategickej, operačnej a taktickej úrovni vytvárajú predpoklady k porazeniu IED systému (viď. Obrázok 3).

Perspektívne z pohľadu NATO je dôležité si uvedomiť, že opatrenia k zníženiu rizika čeliť hrozbe IED musia vzhľadom k vlastnej bezpečnosti krajiny NATO budovať a rozvíjať za pomoci národných spôsobilostí. K týmto spôsobilostiam neoddeliteľne patria vojenské spravodajstvo s prostriedkami exploatácie, ženijné zabezpečenie s jednotkami EOD, ako aj výskum a zavádzanie nový technológii, ktorými budú príslušníci koaličných síl vybavený a kolektívne schopní čeliť hrozbe útokov IED.

Podobne ako člen organizácie NATO aj Slovenská republika identifikuje hrozbu IED ako jednu zo vážnych hrozieb. Hrozba IED je uvedená v zozname identifikovaných hrozieb v základných dokumentoch o bezpečnosti Slovenskej republiky[3].

[3] Aktuálne znenie základných dokumentov riešiacich bezpečnosť Slovenskej republiky je dostupné na stránke https://www.vlada.gov.sk/zakladne-dokumenty-riesiace-bezpecnost-slovenskej-republiky/

NATO oblasť boja proti IED z vojenského pohľadu chápe komplexne, ako funkciu spôsobilostí prospievajúcich k ochrane vlastných síl. K plnohodnotnej realizácii prístupu NATO k boju proti IED je v podmienkach OS SR potrebné implementovať aliančnú doktrínu AJP-3.15 (C) vo forme služobného predpisu OS SR. Spolu s implementáciou AJP-3.15 by mali OS SR vytvoriť funkčný systém boja proti IED prostredníctvom výcviku jednotlivca, udržiavaním a rozvojom vojenských spôsobilostí (vojenské spravodajstvo, ženijné zabezpečenie, EOD) ako aj spoločných vojenských cvičení.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

AJP 3.18 Allied Joint EOD doctrine-study draft, Brussels: NSO forum, August 2021.

AJP-01 Allied Joint doctrine Edition E Version 1, Brussels: NSO, 2017.

AJP-3 Allied Joint Doctrine for the Conduct of Operation Edition C Version 1, Brussels: NSO, 2019. Page 123 – 125,

AJP-3.15 Allied Joint Doctrine For Countering Improvised Explosive Devices Edition C Version Brussels: NSO, 2018.

ATP-3.12.1.1 (B), Allied Tactical Doctrine for Military Search JIEDDO/DIA Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon; 5th Ed, Oct 2017, Page 13-15.

DHS, Department of Homeland Security, IED Attack: Improvised Explosive Devices (Washington, DC: The National Academies Press) 2010. In *Department of Homeland Security*, [online] December 2010 [cit. 29.08.2022]. Dostupné na internete: http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf.

Elektronický lexikón slovenského jazyka, 1987, [online] 1987 [cit. 29.08.2022] Dostupné na internete: http://www.slex.sk.

HOTCHKISS, P. Explosive Threats. In *Explosive Threats - The Challenges They Present and Approaches to Countering Them*, 2018 [online] 01.01.2018 [cit. 29.08.2022] . Dostupné na internete: https://www.osti.gov/servlets/purl/1468512.

MC-0560/2 Policy for Military Engineering, Brussels: NSO forum, 2017.

MICHAUD, Y. The silver bullet: The comprehensive approach to Counter Improvised Explosive Devices, 2013. In *JCSP 39 Master of Defence Studies* [online]. 2013 [cit. 29.08.2022] Dostupné na internete: https://www.cfc.forces.gc.ca/259/290/299/286/michaud_y.pdf.

NATO EOD COE. EOD-IEDD VR-XR Training and Combat Support Kit 2021. In *EOD COE* [online]. 08.12.2021 [cit. 29.08.2022] Dostupné na internete: https://www.eodcoe.org/en/technology-dept/eod/iedd-vr/xr-training-combat-support-kit/.

NATO Term, the official NATO Terminology Database. In *NATO Standardization Office* [online]. 29.08.2022 [cit. 29.08.2022] . Dostupné na internete: https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.

North Atlantic Treaty Organization. NATO Accredited Centres of Excellence NATO COEs catalogue 2021. In *North Atlantic Treaty Organization, E- Library* [online]. 03.11.2020 [cit. 29.08.2022]. Dostupné na internete: https://www.nato.int/cps/en/natohq/topics_77646.htm.

SINGER, P. The evelution of the IEDs, 2012. In *Brookings* [online]. 07.02.2012 [cit. 29.08.2022] Dostupné na internete: http://www.brookings.edu/research/articles/2012/02/improvised-explosive-devices-singer.

SOŠ 3680 AAP-6 Slovník termínov a definícií NATO (vydanie 12), Bratislava, December 2021.

UNAMA. United Nations Assistance Mission in Afghanistan, 2021. In *UNAMA News* [online]. 26.06.2021 [cit. 29.08.2022] Dostupné na internete: https://unama.unmissions.org/civilian-casualties-set-hit-unprecedented-highs-2021-unless-urgent-action-stem-violence-%E2%80%93-un-report.

NATO EOD COE. Integration of the Exoskeleton in the Battlefield Workshop 2017- Calling notice, 2017. In *EOD COE* [online]. 14.7.2017 [cit. 29.08.2022] Dostupné na internete: https://www.eodcoe.org/files/en/events/integration-exoskeleton-battlefield-conference/calling-letter-final-iebws.pdf.

Kalendárium. 24.12.1800 Atentát na Napoleona, 2020. In *Lovec pokladu* [online]. 24.12.2020 [cit. 29.08.2022] Dostupné na internete: https://www.lovecpokladu.cz/home/24-12-1800-atentat-na-napoleona-8364.

pplk. Ing. Alexander HUGYAR, externý doktorand Katedry bezpečnosti a obrany
Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 01 Liptovský Mikuláš, SR
alexander.hugyar@eodcoe.org

SOCIÁLNE SIETE AKO PRIESTOR PRE ŠÍRENIE KONŠPIRAČNÝCH TEÓRIÍ A DEZINFORMÁCIÍ[1]

SOCIAL NETWORKS AS A SPACE FOR THE SPREAD OF CONSPIRACY THEORIES AND DISINFORMATION

Radoslav IVANČÍK

ABSTRACT

The contemporary modern human civilization is significantly influenced by deepening globalization processes, which are manifested to a greater or lesser extent in all spheres of society's life. With one of the manifestations of the current era, closely connected with the dynamic onset of new media, the rapid development and massive use of information and communication technologies, systems and tools, a new range of possibilities has also appeared, such as all kinds of information, news, stories or theories to receive, search, share and spread further. However, at the same time, a new range of possibilities has also appeared, such as modern technologies and devices to be misused and spread through them deceptive, misleading, and distorted information, news, stories, or theories – disinformation and conspiracy theories. The aim of the author of the paper is therefore to point out the danger of the spread of conspiracy theories and disinformation in society through qualitative theoretical interdisciplinary scientific research, to contribute to the increase of education in this area by theoretical and terminological definitions of the subject terms, and simultaneously to clarify the role that social networks play in this area today.

Key words: social networks, conspiracy theories, disinformation, internet

ÚVOD

Súčasná moderná ľudská civilizácia je výrazným spôsobom ovplyvnená prehlbujúcimi sa globalizačnými procesmi, ktoré sa vo väčšej či menšej miere prejavujú vo všetkých sférach života spoločnosti. S jedným z prejavov súčasnej doby, úzko spojenej s dynamickým nástupom nových médií, prudkým rozvojom a masívnym využívaním informačných a komunikačných technológií, systémov a prostriedkov, sa objavila aj nová škála možností ako najrôznejšie informácie, správy, novinky či teórie prijímať, vyhľadávať, zdieľať a šíriť ďalej. Zároveň sa však objavila aj nová škála možností ako moderné technológie a zariadenia zneužiť a šíriť prostredníctvom nich klamlivé, zavádzajúce a skreslené informácie, správy, príbehy či teórie – dezinformácie a konšpiračné teórie – s cieľom ovplyvniť konanie ľudí. Šírenie konšpiračných teórií a dezinformácií, ktoré reagujú na rôzne významné udalosti odohrávajúce sa okolo nás, tak predstavuje veľmi nebezpečnú hrozbu, ktorá môže mať pre jednotlivcov, organizácie i celú ľudskú spoločnosť veľmi nepriaznivé dôsledky.

Čo to vlastne sú konšpiračné teórie a dezinformácie? Ako fungujú, ako sa šíria, prečo sú hrozbou pre jednotlivcov i spoločnosť a prečo im ľudia veria? Hľadaním odpovedí na tieto a ďalšie otázky úzko súvisiace s konšpiračnými teóriami a dezinformáciami sa zaoberá autor príspevku, ktorého cieľom je prostredníctvom kvalitatívneho teoretického interdisciplinárneho vedeckého výskumu, s využitím analyticko-syntetických a komparatívnych prístupov, priblížiť

[1] Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-20-0334.

čitateľom, okrem odpovedí na vyššie uvedené otázky, základné teoretické východiská týkajúce sa skúmania problematiky konšpiračných teórií a dezinformácií a objasniť akú úlohu v tom zohrávajú sociálne siete.

1 ZÁKLADNÉ TEORETICKÉ A TERMINOLOGICKÉ VYMEDZENIE POJMOV KONŠPIRAČNÉ TEÓRIE A DEZINFORMÁCIE

Pojmom, úzko súvisiacim so šírením najrôznejších vymyslených, klamlivých a/alebo pozmenených príbehov a udalostí šírených cestou sociálnych sietí, sú konšpiračné teórie. Čo to vlastne sú tie konšpiračné teórie? Z etymologického hľadiska slovo *„konšpirácia“* pochádza z latinského slova *„conspirare“*, ktoré možno doslova preložiť ako *„dýchať spolu“*, v skutočnosti však tento výraz označuje dvoch alebo viacerých ľudí spriadajúcich plány, o ktorých nikomu nehovoria. Teoreticky, takýto plán nemusí byť hneď zlý, odsúdeniahodný, môže byť aj dobrý, ak napríklad niekto chce niekoho pozitívne, milo prekvapiť. Postupom času ale nadobudlo toto slovné spojenie negatívny význam. Konšpirácie síce nie sú definované ako vyslovene tajné, ale tým, že sa toto slovo spojilo s kriminálnym konaním, tak túto vlastnosť získalo. Takže utajenie sa stalo súčasťou nášho vnímania slova konšpirácia. A súčasť je to veľmi dôležitá, zvlášť ak vezmeme do úvahy jeho vývoj. V princípe sú tak konšpiračné teórie alternatívnym výkladom skutočnosti či histórie, keďže nič sa podľa nich, resp. konšpirátorov nedeje zo zjavných dôvodov, ale preto, že to bolo vopred niekým tajne naplánované (Greig, 2019, s. 6).

Podstata konšpiračných teórií tým pádom spočíva v tom, že nič nie je také, ako sa na prvý pohľad zdá, a že všetko so všetkým spolu súvisí. Inými slovami povedané, konšpiračné teórie sa snažia presvedčiť ľudí, že existuje určitá skupina ľudí – sprisahancov, ktorí tajne plánujú a organizujú všetko, čo sa deje. Vymyslených sprisahancov zvyčajne prezentujú ako nepriateľov ľudu. Konšpiračné teórie tak rozdeľujú svet na dobro a zlo, na My verzus Oni. Tvrdia, že ľudia sa musia pozrieť pod povrch, aby odhalili činy a zámery sprisahancov, ktorí vynakladajú veľké úsilie, aby skryli svoje zlé zámery. Predpokladom je, že ak ten alebo tí, ktorí chcú vedieť, ako to naozaj je alebo bolo, teda vedieť „skutočnú pravdu“, musia „vŕtať, kopať, ryť“ dostatočne hlboko, aby objavili skryté prepojenia medzi ľuďmi, inštitúciami a udalosťami, ktoré vysvetľujú, čo sa v skutočnosti deje alebo stalo (Quassam, 2019).

Tieto predpoklady prirodzene stavajú konšpiračné teórie do rozporu s modernou vedou, ktorá zdôrazňuje dôležitosť náhody, možnosť zhody náhod, možnosti výskytu nepredvídaných okolností a nezamýšľaných dôsledkov. Konšpiračné teórie naopak naznačujú, že významné udalosti sú vždy výsledkom ich tajného, zámerného, sprisahaneckého plánovania a ovplyvňovania. Na druhej strane si je ale potrebné v tejto súvislosti uvedomiť, že konšpiračné teórie väčšinou nevznikajú len tak odnikiaľ, resp. len tak z ničoho nič. Často sú reakciami – aj keď zjednodušenými a skreslenými – na skutočné problémy vyskytujúce sa v spoločnosti (Uscinksi – Parent, 2014).

Konšpiračné teórie pritom nie sú ničím novým, sú tu už tisícky rokov, o tom nie sú žiadne pochybnosti. Koniec koncov samotné konšpirácie existujú už poriadne dlho. Príkladom môžu byť viaceré udalosti, ako napríklad plán starovekých Grékov obsadiť Tróju, alebo sprisahanie nepriateľov Gaia Julia Caesara vedúce k jeho vražde a ďalšie. História je takýchto dramatických konšpirácií naozaj plná. A spolu s nimi tu boli vždy aj podozrievaví ľudia, ktorí vždy prišli s nejakou sprisahaneckou konšpiračnou teóriou, ktorá tajuplné udalosti „vysvetlila“ a ukázala ľuďom „ako to naozaj v skutočnosti bolo“. V tých časoch bolo z pochopiteľných dôvodov šírenie konšpiračných teórií značne obmedzené. Navyše, v minulosti ľudia mnohé javy a udalosti vnímali ako zásah bohov. Preto sa konšpiračné teórie dostali do povedomia väčšieho počtu ľudí až v minulom storočí, čo pravdepodobne súvisí nielen s rozvojom tlače, médií a technológií, ale aj s určitým úpadkom viery. V sekulárnejších časoch totiž ľudia začali

byť náchylnejší viac veriť tomu, že významné udalosti sa odohrali tak preto, že išlo o tajné, zlomyseľné sprisahanie mocných a nie zásah božstiev. Náhľad na svet, ktorý ovláda malá, utajená skupina ľudí – elita – je pretrvávajúcim prvkom aj dnešných konšpiračných teórií. V podstate sa dá povedať, že táto skupina stojí za takmer každou konšpiračnou teóriou, ktorá sa dnes zdieľa medzi ľuďmi či už prostredníctvom sociálnych sietí alebo akýmkoľvek iným spôsobom. Takže odpoveďou na otázku, čo je konšpiračná teória by mohlo byť: *„Je to teória, ktorá naznačuje, že veľké, významné udalosti nie sú tým, čím sa zdajú byť, ale manifestáciou sveta ovládaného utajenou elitou"* (Greig, 2019, s. 7).

Dezinformácie sú, podobne ako mnohé iné pojmy, definované rôzne. V súčasnosti neexistuje žiadne ich jednotné, unifikované a všeobecne akceptované definičné vymedzenie a tak sa v literatúre môžeme stretnúť s pomerne veľkým množstvom definícií líšiacich sa predovšetkým tým, v akom odvetví či oblasti spoločnosti sa dezinformácie vyskytujú, resp. aplikujú. Napriek ich väčšej či menšej odlišnosti, spoločným rysom všetkých používaných definícií je fakt, že ide o úmyselnú modifikáciu poskytovaných informácií so zámerom ovplyvniť, oklamať či uviesť adresátov týchto informácií do omylu.

V slovenskom prostredí sú pomerne často využívané definície nachádzajúce sa v príslušných slovníkoch. Napríklad v Slovníku cudzích slov (2015) je dezinformácia vymedzená veľmi stručne ako „*nesprávna, vedome skreslená informácia*". V Slovníku súčasného slovenského jazyka (2015) je už dezinformácia definovaná obšírnejšie ako „*nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu*". V Slovníku pojmov z mediálnej výchovy (2020) sa uvádza, že „*dezinformácia je úmyselne nesprávna či skreslená informácia tajne implantovaná do informačnej sústavy oponenta so zámerom ovplyvniť potrebným smerom jeho aktivity*".

Národný bezpečnostný úrad (2021) na margo definovania dezinformácií uvádza, že tento pojem zatiaľ nebol v Slovenskej republike kodifikovaný, a preto sú v literatúre a príslušných dokumentoch väčšinou uvedené definície prevzaté z odborných publikácií či oficiálnych európskych dokumentov, ktoré sú si podobné a vystihujú podstatu pojmu. Zároveň dodáva, že „*dezinformácie môžu byť súčasťou širšieho procesu informačného ovplyvňovania, ktorý sa označuje pojmom informačné operácie*".

V českom prostredí, v Sociologickej encyklopédii (2017) je dezinformácia definovaná ako „*akákoľvek skreslená, falošná informácia, používaná s cieľom ovplyvniť jednotlivca aj určitú skupinu ľudí určitým žiaducim spôsobom. Väčšinou ide predovšetkým o vyvolanie dobrého či zlého dojmu o nejakej osobe, udalosti, diele, jave, rokovaní a pod. v záujme politickom, ideologickom alebo aj rýdzo súkromnom. Často je zameraná na ovplyvnenie verejnej mienky, pričom môže byť s takým zámerom už vytvorená, ale môže vzniknúť aj náhodne alebo za iným účelom, ktorý nemusí byť vyslovene dezinformačný (napr. keď je spôsobená vytrhnutím určitého oznámenia z pôvodného kontextu, resp. jeho zasadením do iného kontextu)*".

Na doplnenie vyššie uvedených definícií možno uviesť, že v anglofónnom jazykovom prostredí sa môžeme stretnúť tiež s viacerými vymedzeniami pojmu dezinformácia. Napríklad v Oxfordskom anglickom výkladovom slovníku (2021) je dezinformácia definovaná stručne ako „*úmyselne poskytovaná falošná informácia*", v Cambridgeskom slovníku anglického jazyka (2021) ako „*nepravdivá informácia šírená s cieľom oklamať ľudí*", a v MacMillanovom výkladovom slovníku (2019) ako „*nepravdivá informácia, ktorá má presvedčiť ľudí, aby verili niečomu, čo v skutočnosti nie je pravda*".

Dezinformácie je možné rozlíšiť z niekoľkých hľadísk. Z pohľadu ich tvorby a prejavu ich možno rozdeliť na a) pasívne a b) aktívne. Pasívne dezinformácie spočívajú v zatajení, zadržaní alebo oneskorení informácie s cieľom navodenia mylného dojmu. Aktívne dezinformácie reprezentujú, ako vyplýva z ich označenia, aktívnu tvorbu nepravdivých

informácií alebo modifikáciu pôvodných informácií či ich kontextu. Ide o ich priamu aktívnu falzifikáciu. Z hľadiska cieľov je možné dezinformácie rozdeliť na a) strategické, ktorých použitím sa sleduje určitý dlhodobý strategický cieľ, napríklad nastolenie nejakého nového usporiadania, poriadku a pod., a b) taktické, ktorých využitie má operatívny charakter a slúži k postupnému napĺňaniu vytýčených dlhodobých cieľov (Neumannová, 2017).

Z vyššie uvedených informácií jednoznačne vyplýva, že za hlavný znak dezinformácie možno považovať to, že ide o úmyselné konanie, a to tak v prípade pasívnej formy, kedy dochádza k úmyselnému zatajovaniu správ či ich pozdržaniu, ako aj v prípade aktívnej formy, kedy sa informácie aktívne vytvárajú alebo upravujú podľa stanoveného zámeru.

Pre lepšie pochopenie pojmu dezinformácia, pre jeho správne používanie a vyhnutie sa zamieňaniu s inými podobnými pojmami, predovšetkým s pojmom misinformácia, je potrebné vysvetliť aspoň základný rozdiel medzi týmito dvomi pojmami. Kým v prípade dezinformácie, ako už je uvedené vyššie, ide o úmyselné konanie s cieľom zaviesť, pomýliť, oklamať ľudí alebo presvedčiť ich, aby verili niečomu, čo nie je pravda, tak v prípade misinformácie tento úmysel chýba. Je to síce nesprávna alebo zavádzajúca informácia, avšak nie je šírená ani systematicky, ani úmyselne, ani s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ju prijímajú. Napriek tomu, hoci ide o neúmyselný akt, môže mať misinformácia v konečnom dôsledku rovnaký vplyv na obyvateľov ako dezinformácia, a teda ovplyvniť názory cieľovej skupiny na základe nepravdivej správy.

2 SOCIÁLNE SIETE AKO PRIESTOR PRE ŠÍRENIE KONŠPIRAŠNÝCH TEÓRIÍ A DEZINFORMÁCIÍ

Základným cieľom všetkých konšpiračných teórií a dezinformácií je pokúsiť sa ovplyvniť skutočných ľudí. Pre naplnenie tohto cieľa je potrebná stratégia, ktorá zahŕňa široké spektrum jednotlivých krokov, ktoré je potrebné naplánovať pre dosiahnutie požadovaného úspechu. Pre šíriteľa/šíriteľov je veľmi dôležité stanovenie konkrétnej cieľovej skupiny, ktorú majú konšpiračné teórie alebo dezinformácie zasiahnuť, a vybrať vhodný obsah korešpondujúci s vytýčeným cieľom. Jedným z hlavných elementov je voľba vhodných prostriedkov, ktoré majú byť využité pre konšpiračné alebo dezinformačné účely. Primárnou platformou pre šírenie konšpiračných teórií a dezinformácií je síce v súčasnej dobe internet, v ktorého sieti šírenie sprostredkovávajú najmä najrôznejšie sociálne siete alebo dezinformačné weby, ale skreslené, nepravdivé, vymyslené a klamlivé informácie, správy, teórie či príbehy sa objavovali a objavujú v podstate v akýchkoľvek mediálnych kanáloch a šíriť sa môžu aj ústne. V súčasnosti sú to ale bezpochyby predovšetkým sociálne siete, ktoré poskytujú šíriteľom priestor na šírenie rôznych konšpiračných teórií a dezinformácií.

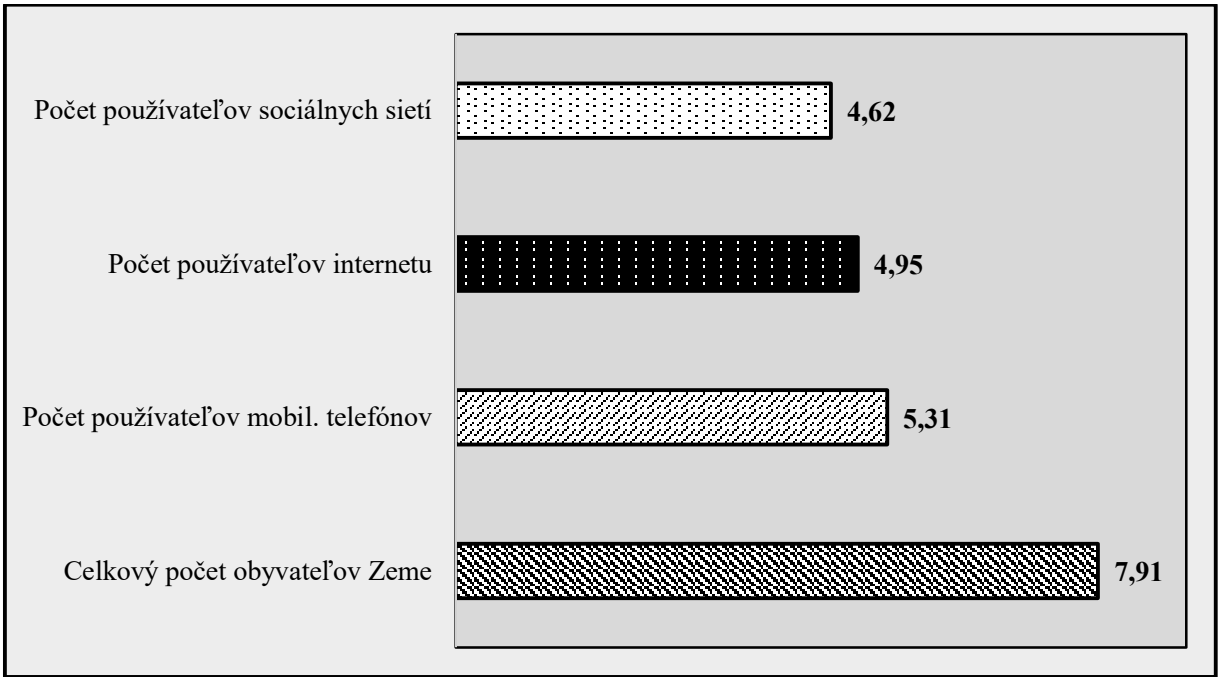
Používanie rôznych lží alebo prekrúcanie faktov za účelom ovplyvnenia jednotlivcov alebo aj celej verejnosti nie je teda žiadnou novinkou, ak sa však spojí so sofistikovanými prostriedkami, aké predstavujú dnešné moderné, tzv. „smart“ prostriedky a technológie, s prostredím sociálnych sietí a internetu, prípadne aktivitou hackerov, objavuje sa tu nová a veľmi silná hrozba šírenia dezinformácií, ktoré môžu predstavovať nebezpečenstvo nielen pre jednotlivcov a organizácie, ale v niektorých prípadoch bezpečnostnú hrozbu pre národnú i medzinárodnú bezpečnosť.[2]

Vznik a rýchly rozvoj sociálnych médií viedol k radikálnej zmene spôsobov, akými ľudia komunikujú a získavajú informácie. Tento nový spôsob komunikácie sa vyznačuje veľmi vysokou rýchlosťou s akou sa správa prenáša. Sociálne médiá tiež ponúkajú najvyšší stupeň interakcie, aký môžu aktuálne komunikačné prostriedky používateľom poskytovať. Prístup k informáciám je takmer neobmedzený a lacný, zväčša úplne zadarmo. Taktiež nedostatok fóra

[2] Na narušenie bezpečnosti vplýva okrem dezinformácií množstvo ďalších faktorov, ktoré sú navzájom nezávislé a neustále sa vyvíjajú (Bučka – Andrassy, 2017).

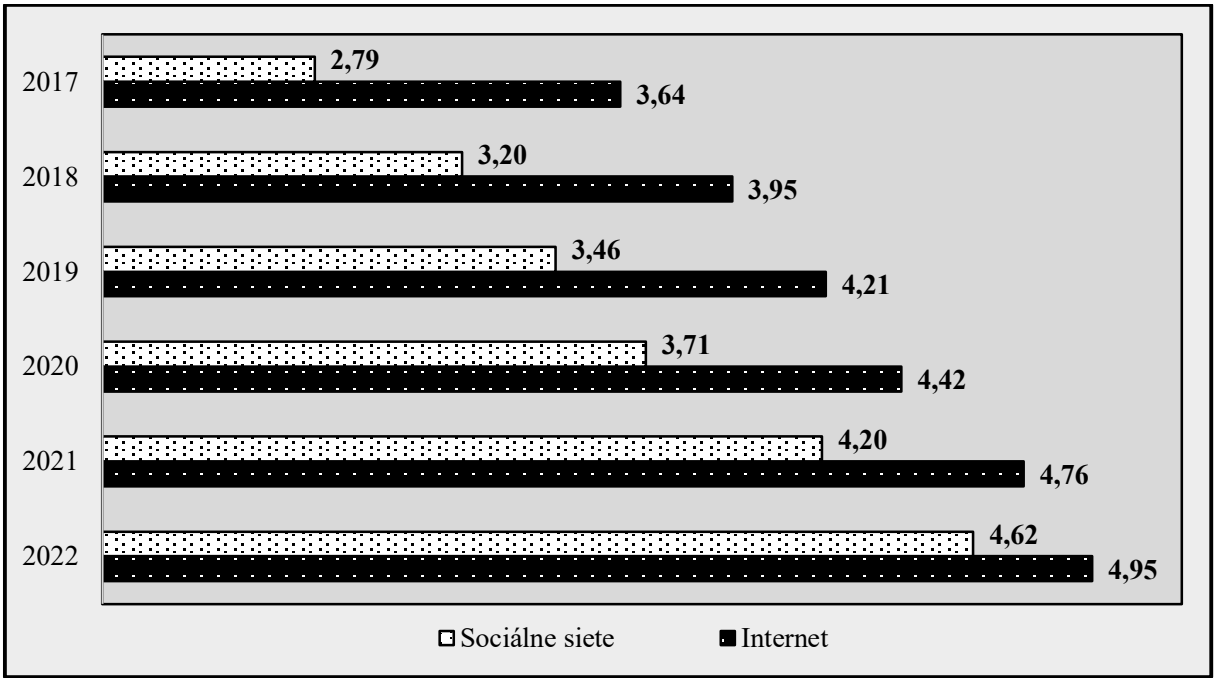
na reguláciu online obsahu, na rozdiel od toho, ktorý sa vysiela prostredníctvom tradičných mediálnych kanálov, robí online prostredie sociálnych sietí mimoriadne tolerantným.

Čo sa týka penetračnej kapacity platforiem sociálnych médií, poskytnuté štatistické údaje z januára 2022 poukazujú na značný nárast používania sociálnych sietí v porovnaní s predchádzajúcimi rokmi, ale aj na prognózu pokračovania tohto trendu. Podľa aktuálnych informácií mobilný telefón používa dnes cca 5,31 miliardy obyvateľov, čo predstavuje viac ako dve tretiny (67,1 %) svetovej populácie, internet používa približne 4,95 miliardy ľudí, teda viac ako tri pätiny (62,5 %) svetovej populácie, a počet aktívnych používateľov sociálnych sietí dosahuje zhruba 4,62 miliardy, čo predstavuje podiel na celkovom obyvateľstve planéty na úrovni 58,4 % (graf 1). Sociálne siete používa pritom prostredníctvom mobilného telefónu až 95 % ich užívateľov (DR, 2022).



Graf 1 Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí v roku 2022 na celom svete (v mld.)
Zdroj: DR, 2022

O tom, aký dynamický je rast používateľov internetu a sociálnych sietí svedčí fakt, že za ostatných päť rokov celosvetovo stúpol počet používateľov internetu o viac ako jednu tretinu (o 36 %). Kým v roku 2017 používalo internet zhruba 3,64 miliardy ľudí, tak v roku 2022 to už bolo približne 4,95 miliardy. Rast používateľov sociálnych sietí je ešte dynamickejší, nakoľko stúpol v hodnotených rokoch o takmer dve tretiny (o 65,6 %). Kým v roku 2017 používalo sociálne siete približne 2,79 miliardy ľudí, v roku 2022 sú to už zhruba 4,62 miliardy (graf 2). Z nich jeden užívateľ strávi na sociálnych sieťach priemerne denne 2 hodiny a 27 minút a priemerne mesačne využíva 7,5 rôznych sociálnych sietí (DR, 2022).



Graf 2 Prehľad rastu používateľov internetu a sociálnych sietí v rokoch 2017 až 2022 (v mld.)
Zdroj: DR, 2022

Dynamika a komplexnosť sociálnych sietí spôsobuje, že spoločnosť musí čeliť novým typom bezpečnostných rizík a hrozieb. Šíritelia konšpiračných teórií a dezinformácií totiž využívajú a zároveň zneužívajú mechanizmy sociálnych médií uverejňovaním zavádzajúcich, klamlivých, skreslených či doslova vymyslených nepravdivých informácií, správ, príbehov alebo teórií. Sociálne siete by pritom mali poskytovať neutrálne prostredie na vyjadrenie názorov. Ale je to skutočne tak? Veď už len základná koncepcia odmeňovania lajkami a zdieľaniami podporuje vznik prejavov vyjadrujúcich úžas, začudovanie, pobúrenie, škandál alebo rozruch či senzáciu, pričom pozitívna spätná väzba na takéto príspevky podporuje tvorbu ďalších. Takéto „stimuly" na sociálnych sieťach potom menia spôsob, akým sa ľudia vyjadrujú a akým pridávajú príspevky. Ak príspevok vzbudzujúci úžas, začudovanie, škandál, pobúrenie, senzáciu alebo rozruch nad nejakou udalosťou, javom, situáciou a pod. dostane viac lajkov a zdieľaní ako „bežný" príspevok, používateľov sociálnych sietí to zväčša podnecuje k pridaniu ďalších príspevkov podobného charakteru a ich zdieľaniu. Takéto odmeňovanie cestou sociálnych sietí vytvára slučky pozitívnej spätnej väzby, ktoré podporujú vytváranie, prijímanie, zdieľanie a šírenie rôznych konšpiračných teórií a dezinformácií.

Výrazný vplyv na túto situáciu stále má aj tzv. koronakríza vyvolaná pandémiou koronavírusu spôsobujúceho ochorenie Covid-19[3]. Ovplyvňuje všetkých, ako jednotlivcov, tak aj sociálne skupiny. S postupným nárastom izolácie narastalo aj používanie sociálnych sietí a čas strávený pred obrazovkami počítačov, tabletov či mobilných telefónov. Nie je to len preto, že sociálne siete a digitálne nástroje môžeme na prvý pohľad považovať za záchranu v čase karantény a sociálneho dištancovania sa, ale tiež z dôvodu, že na sociálnych sieťach možno jednoducho a rýchlo nájsť takmer všetky nové informácie (nielen) o aktuálnej situácií.

[3] V čase spracovania príspevku (k 7.7.2022) bolo celosvetovo infikovaných koronavírusom 553 710 910 ľudí, pričom ochoreniu Covid-19 podľahlo 6 348 219 osôb. V Slovenskej republike bolo k uvedenému dátumu evidovaných 1 799 763 infikovaných osôb, z ktorých zomrelo 20157 ľudí (John Hopkins Coronavirus Resource Center, 2022).

ZÁVER

V ostatných rokoch sa aj z dôvodu dynamického vývoja ľudskej spoločnosti v oblasti informačných a komunikačných technológií, systémov a prostriedkov výrazne mení náš spôsob sociálneho fungovania. V posledných dvoch rokoch sa na tejto zmene zásadným spôsobom podieľa aj pandémia koronavírusu a prijímané opatrenia zamerané na elimináciu jeho šírenia a ochranu verejného zdravia. Zo spoločenského tvora, akým človek je, sa stáva tvor „sociálno-sieťový“. Sociálne siete totiž predstavujú neraz jediný spôsob, ako sa s niektorými ľuďmi „stretávame“, ako spoznávame názory iných, ako komunikujeme.

Postupujúca internetizácia, informatizácia a digitalizácia spoločnosti, ako aj s nástup nových médií a masívne využívane sociálnych sietí prinieslo množstvo pozitív, ale aj viaceré negatíva. Tie zvyčajne súvisia s anonymitou na sociálnych sieťach, s prekrúcaním reality alebo s ukazovaním nereálnych cieľov a hodnôt, ktoré by hodnotami ani byť nemali. Sociálne siete, ako ukazujú vyššie uvedené údaje, sa stali pevnou súčasťou každodenného života mnohých ľudí. Stali sa veľmi silným informačným a komunikačným nástrojom, ktorý zmenil spôsob medziľudskej komunikácie.

Nie je na tom nič divné, pretože naozaj prinášajú veľa pozitív, môžeme sa napríklad porozprávať so spolužiakom / spolužiačkou zo základnej, strednej či vysokej školy alebo kamarátom / kamarátkou z detstva, ktorého / ktorú sme viac rokov nevideli, zistiť, čo zaujíma osobu, ktorá sa nám páči, a podobne. Sociálne médiá tiež výrazne urýchľujú tok informácií, dát, šírenie myšlienok a nápadov. Z pozitívnych efektov možno spomenúť aj rôzne podporné skupiny pre ľudí, ktorí majú rôzne zdravotné problémy či patria do menšinovej komunity, pomoc pri vzdelávaní alebo pri poskytovaní priestoru pre kreativitu či sebavyjadrenie, samozrejme, ak sa použijú správne.

Žiaľ, sociálne siete a ich masové využívanie a v mnohých prípadoch aj zneužívanie má aj svoje tienisté stránky a nie je ich málo. Existujú dôkazy, že nadmerné používanie týchto novodobých médií môže mnohými spôsobmi negatívne ovplyvniť duševné zdravie. Viaceré prieskumy vo viacerých krajinách ukázali, že niektorí ľudia trávia na sociálnych sieťach neraz 9 až 11 hodín denne a postupne začínajú žiť „mimo reality“. Ľudia, ktorí používajú sociálne médiá viac ako 2 hodiny denne, majú oveľa väčšiu pravdepodobnosť problémov duševného zdravia. Väčšina ľudí, ktorí trávia na sociálnych sieťach niekoľko hodín denne má problémy so spánkom, trpí depresiami, zažíva úzkostné stavy, má pocit menejcennosti. Ďalším z veľmi nebezpečných negatív sociálnych sietí je to, že poskytujú príležitosť anonymne šíriť rôzne konšpiračné teórie a dezinformácie, ktoré môžu veľmi nepriaznivo ovplyvniť konanie a správanie ľudí, narúšať existujúce demokratické hodnoty, fungovanie demokratických inštitúcií a tým ohroziť aj celú spoločnosť.

Aj preto je veľmi dôležité zo strany štátu a jeho kompetentných inštitúcií podporovať prevenciu a vzdelávanie v oblasti mediálnej gramotnosti a práce s informáciami. Zvýšenie povedomia o konšpiračných teóriách a dezinformáciách, zlepšenie schopnosti rozoznávať a odhaľovať ich, ako aj eliminovať ich šírenie v čo najväčšej miere by určite znamenalo menej príležitostí napríklad pre populizmus, radikalizmus, extrémizmus, xenofóbiu či rozdeľovanie spoločnosti. Angažovanie štátu v tejto problematike je z toho dôvodu nielen žiaduce, ale dokonca nevyhnutné. Na druhej strane si všetci musíme uvedomiť, že možnosti štátu nie sú nekonečné, nie všetko za nás vyrieši štát, a tak je nutné, aby sme aj my sami prispeli k potláčaniu množstva, sily a vplyvu konšpiračných teórií a dezinformácií a ich šíriteľov na naše životy.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

GREIG, C. 2019. *Konspirační teorie*. Brno : CPress, 2019. 128 s. ISBN 978-80-264-2831-2.

QASSAM, C. 2019. Conspiracy Theories. Cambridge : Polity Press, 2019. 140 s. ISBN 978-1-5095-3583-5.

USCINSKI, J. E. – PARENT, J. M. 2014. American Conspiracy Theories. Oxford : Oxford University Press, 2014. 221 s. ISBN 978-0-199-35181-7.

BUČKA, P. – ANDRASSY, V. 2017. Distributed simulation as a platform of security community preparation, In *Distance Learning, Simulation and Communication 2017: CD proceedings.* Brno : University of Defence, 2017. ISBN 978-80-7231-416-4.

Cambridge Dictionary. 2021. *Disinformation*. [online] Dostupné na: <https://dictionary.cambridge.org/dictionary/english/disinformation>

DR. 2022. Global Digital Overview. In DataReportal, 2022. [online] Dostupné na internete: <https://datareportal.com/reports/digital-2022-global-overview-report>.

Macmillan Dictionary. 2021. *Disinformation*. [online] Dostupné na internete: <https://www.macmillandictionary.com/dictionary/british/disinformation>.

NBÚ. 2021. *Dezinformácie a informačné operácie*. [online] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html>

NEUMANNOVÁ, Š. 2017. *Dezinformace*. [online] Dostupné na: <https://encyklopedie.soc.cas.cz/w/Dezinformace>

Oxford Dictionary. 2021. *Disinformation*. [online] Dostupné na internete: <https://www.oxfordlearnersdictionaries.com/definition/english/disinformation?q=disinformation>

Slovník cudzích slov. 2015. *Dezinformácia*. [online] Dostupné na internete: <https://slovnik.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=bernolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>

Slovník pojmov z mediálnej výchovy. 2020. *Dezinformácia.* [online] Dostupné na internete: <https://medialnavychova.sk/dezinformacia/>

Slovník súčasného slovenského jazyka. 2015. *Dezinformácia.* [online] Dostupné na internete: <https://slovnik.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=bernolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>

Sociologická encyklopedie. 2017. *Dezinformace*. [online] Dostupné na internete: <https://encyklopedie.soc.cas.cz/w/Dezinformace>

JHCRC. 2022. COVID-19 Dashboard. In *John Hopkins Coronavirus Resource Center*. [online] Dostupné na internete: <https://coronavirus.jhu.edu/map.html>

plk. gšt. v. z. doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 935 17 Bratislava
radoslav.ivancik@akademiapz.sk

THE ALLIANCE'S PARTNERSHIPS IN THE LIGHT OF THE MADRID SUMMIT

Klára SIPOSNÉ KECSKEMÉTHY, Alexandra SIPOS

ABSTRACT

The Madrid Summit was of particular importance for NATO moving forward towards credible defence and enhanced deterrence. This paper reviews the road leading up to the Madrid Summit and the formulation of the new Strategic Concept. The Russian invasion of Ukraine on 24 February 2022 radically changed the security environment. The summit focused on the challenges, risks and threats on the eastern and southern borders of the Alliance, the response to these, border protection, the NATO-Russia relationship and military capabilities. This paper deals with the historic decisions taken by NATO in the context of the partnership, the invitation of Finland and Sweden and the priority given to the Asia-Pacific region, the Madrid Summit developments in partnership relations.

Keywords: Madrid Summit; enhanced defence and deterrence; Russian Federation, partnership initiatives, Finland, Sweden, Asia-Pacific region

INTRODUCTION

The Summits play an important role in NATO's life, setting direction, providing guidance, speeding up decision-making and signalling important, historic events. In the post-bipolar era, the rapidly changing security environment and events on the European, Asian and African continents have accelerated the frequency of summit meetings. This was particularly true for 2022. Russia's invasion of Ukraine on 24 February 2022 was a real shock for the Allies. Despite the obvious omens, they could not believe that Russia would attack sovereign, independent Ukraine in flagrant violation of international law.

The 2022 Madrid Summit was historic in many ways. Never before in NATO's history have three summits been held in one year. In 2022, on 25 February, the day after the Russian invasion, NATO heads of state and government met in virtual space.[1] NATO issued a statement after the extraordinary North Atlantic Council meeting „…We are now making significant additional defensive deployments of forces to the eastern part of the Alliance. We will make all deployments necessary to ensure strong and credible deterrence and defence across the Alliance, now and in the future. Our measures are and remain preventive, proportionate and non-escalatory."[2]

This was followed by the in person Brussels Summit on 24 March 2022,[3] and the summit in Madrid on 28-30 June, which went ahead as planned and on schedule. Already in 2021, it was clear that the fourth strategic concept for the post-bipolar era would be negotiated and adopted in Madrid. The Madrid Summit was exceptional because, unlike the enlargement rounds of the post-bipolar period, the preparations for the enlargement round – Finland and

[1] Extraordinary virtual summit of NATO Heads of State and Governments, [online]. Available on internet: https://www.nato.int/cps/en/natohq/events_192464.htm

[2] Statement by NATO Heads of State and Government on Russia's attack on Ukraine, [online]. Available on internet: https://www.nato.int/cps/en/natohq/official_texts_192489.htm, Press conference by NATO Secretary General Jens Stoltenberg following the extraordinary virtual summit of NATO Heads of State and Government, [online]. Available on internet: https://www.nato.int/cps/en/natohq/opinions_192455.htm

3 Statement by NATO Heads of State and Government, Brussels, 24 March, 2022. [online]. Available on internet: https://www.nato.int/cps/en/natohq/official_texts_193719.htm

Sweden – were taking place at an incredible pace.

The Madrid Summit has been the subject of a number of analyses. The most important decisions of the summit were analyzed for deterrence and defence, including the strengthening of the Eastern flank, NATO's military reinforcement after the Russian invasion of Ukraine, transatlantic solidarity and proportional burden sharing, and the reform of the command and control system, the development of the Alliance's response capabilities, decisions on long-term deterrence and defence tasks, and possible future plans for the development of a new NATO force structure.[4]

This paper focuses on the historic NATO partnership decisions, the invitations to Finland and Sweden, and the importance of the Asia-Pacific region, the developments in Madrid in the Alliance's partnership.

1 PREPARATION OF THE NEW STRATEGIC CONCEPT

In preparation for the Madrid Summit, on 31 March 2020, the NATO Secretary General asked experts (Reflection Group) to examine NATO's current situation and future role.[5] They were mandated to make proposals to strengthen the unity, solidarity and cohesion of the Alliance, the transatlantic bond and political consultation between Member States,[6] the reinforcement of NATO's political role and relevant instruments to address threats and challenges to security from all strategic directions was analysed.[7] According to their assessment NATO must adapt to a more complex strategic environment characterised by geopolitical rivalry, confrontation with the Russian Federation, the rise of China and the increasing role of emerging and disruptive technologies, as well as a range of transnational threats and risks. According to the report, cooperation with China is both an opportunity and a challenge, but the report only addresses the latter.

The report „NATO 2030: United for a New Era" made a number of recommendations to the Allied decision-makers, but not all of them were included in the new strategic concept adopted in Madrid. The report's defining chapter is „Recommendations: strengthening NATO's role, cohesion and consultation", which covers political consultation among member countries, with the European Union as the most important ally, and with partner countries.[8] The NATO 2030 report devoted space to debates within the Alliance.[9] The Russian invasion of Ukraine on

---

[4] WAGNER, Péter: A madridi NATO-csúcs kérdései, *Külügyi és Külgazdasági Intézet Elemzések*, 2022. 32. pp. 1–13. [online]. Available on internet: https://kki.hu/wp-content/uploads/2022/07/KKIElemzesek.KE-2022.32.pdf STEPPER, Péter: Az arányos teherviselés és alkalmazkodás kérdései a madridi csúcs előtt. *Külügyi és Külgazdasági Intézet Elemzések*, 2022. 35. p. 1–11. [online]. Available on internet: https://kki.hu/wp-content/uploads/2022/07/KE_2022_35_ES_teherviseles_alkalmazkodas_Nato_SP_0707.pdf; CSIKI VARGA, Tamás–TÁLAS, Péter: Megerősített elrettentés és védelem. Stratégiai Védelmi Kutatóintézet, Elemzések 2022/8. 2022. július 12.; GYARMATI, István: Egy új biztonsági rendszertelenség felé a NATO: Szép új világ. Political Capital, 2022. június 29. [online]. Available on internet: https://www.politicalcapital.hu/hireink.php?article_read=1&article_id=3025; SZENES, Zoltán: Elrettentés és védelem a NATO új haderőmodellje, a Hadtudomány c. folyóirat 2022. 2. számában megjelenő tanulmány.

[5] In December 2019, at the NATO Heads of State and Government meeting in London, Jens Stoltenberg, NATO Secretary General, was asked to launch a comprehensive self-assessment proces (Forward-Looking Reflection Process). Secretary General appoints group as part of NATO reflection process, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_174756.htm

[6] NATO 2030: United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General, Brussels, 25 November 2020. [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

[7] NATO 2030: United for a new era p. 11. See also Globális reformokra készül a NATO Donald Trump „korszaka" és a megjegyzések után? [online]. Available on internet: http://politic.karpat.in.ua/?p=14856&lang=hu

[8] NATO 2030. pp. 53–57.

[9] During the Cold War, there were several internal disputes within the Alliance. This was the case in 1951 during the first group of experts known as the "Three Wise Men", in 1956 during the work of the second "Three Wise Men" Commission, and in the Harmel Report on the future tasks of the Alliance. The post-bipolar era has also been marked by a series of debates, with one of the Alliance's greatest challenges being the scarcity of resources,

24 February 2022 forged the Allies into an unprecedented unity. Thus, the proposals/recommendations made in the new Strategic Concept on the discussions and consensus have not become part of the strategic concept.

The TAG NATO shadow strategic concept 2022: Preserving peace, protecting people is another important preparatory document for the Madrid Summit strategic concept.[10] The most important part of the document is the section on the Alliance's core tasks and responsibilities, in which, in addition to the modernisation of NATO's force structure, effective crisis management, arms control, disarmament and non-proliferation, the section on partnership and the open-door policy is of particular importance. Partnership can lead to full membership through an open door policy, but partnership can be the ultimate aim.

The NATO shadow strategic concept underlined that the Arctic and Northern Europe is becoming an increasingly contested area. As an Arctic country, Canada is directly affected by climate change and the growing Chinese and Russian presence in the region. The Alliance supports the efforts of Canada and Norway to ensure that the Arctic remains a region of peace and exploration and to resist efforts to militarise the region and claims that go beyond the current demarcation agreements. The study confirms that NATO continues to prioritise support for Georgia and Ukraine. NATO will continue its efforts towards the Enhanced Partners, part of the Partnership Interoperability Initiative launched at the Wales Summit.[11] Australia, Finland, Sweden, Georgia, Ukraine and Jordan have developed a tailored partnership with NATO to promote effective interoperability between their armed forces and those of the Alliance. The document reaffirmed that Finland and Sweden are reliable partners in ensuring the integrity of the Euro-Atlantic area, and that their partnership is particularly important to the Alliance because it serves as a model for the closest partnership that has been developed, without membership. [12]

The two documents of the Madrid Summit, the Strategic Concept and the Summit Declaration, [13] set out the policy orientations of the North Atlantic Alliance and its responses to the current situation. The Strategic Concept for 2022 emphasises the general principles of an open-door policy under the heading of cooperative security, focusing on partnership relations, the development of relations with Ukraine, Georgia and Bosnia and Herzegovina in the Euro-Atlantic area, and the strategic partnership with the European Union, political consultation and cooperation priorities (military mobility, resilience, the impact of climate change on security, emerging and disruptive technologies, human security, the women, peace and security agenda, cyber and hybrid threats, the challenge of emerging China). China is included in the strategic concept for the first time. A separate section deals with the country's ambitions and coercive policies, which pose a systemic challenge to the interests, security and values of the Alliance (malign hybrid and cyber operations, confrontational rhetoric, disinformation operations, control of key technological and industrial sectors, critical infrastructures and strategic raw materials and supply chains, undermining the international legal order in space, oceans and cyberspace, etc.).[14] Of particular concern is the deepening strategic partnership between China and Russia. The strategic concept also addresses regions of strategic importance: the Western Balkans, the Black Sea, the Middle East, North Africa, the Sahel, the Indo-Pacific.

---

the decline in defence budgets and the disparity between the defence investments of US and European member states. Robert Gates, among others, made this point in 2011, Donald Trump at the 2017 NATO Summit in Brussels, and French President Emmanuel Macron expressed his doubts in November 2019.

[10] The TAG NATO shadow strategic concept 2022: Preserving peace, protecting people, February 2022. p. 22.

[11] Wales Summit Declaration, 2014. [online]. Available on internet: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[12] The TAG NATO shadow strategic concept 2022, p. 13.

[13] NATO 2022 Strategic Concept, [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf; Madrid Summit Declaration, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, [online]. Available on internet: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

[14] NATO 2022 Strategic Concept 13. and 45. points

2 NATO AND ASIA-PACIFIC PARTNERS

Cooperative security – assessment of cooperation with partners – was an important part of the NATO 2030 report. The majority of partner countries share the Alliance's core values of democracy, freedom and the rule of law, [15] contribute to international peace and stability and to the success of Alliance operations, and address security problems in their respective regions. [16]

The report also highlighted the importance of developing closer cooperation with global partners in the Pacific. Global Partners (GPs) are those states that are not members of the organisation and do not participate in any of the institutionalised partnership fora. They are in an exceptional position, given the importance of their relationship with the North Atlantic Treaty Organisation, but no permanent body or institution has yet been established to provide a space for structured dialogue between the parties. These partners have long-standing interests and links, primarily with the United States of America.

The Global Partners are different from other NATO partnership initiatives (PfP, MD, ICI), in their case we cannot speak of a single Alliance policy, but of individual partnerships with the Alliance. NATO meets regularly with the Asia-Pacific partners, there are recurring consultations in the North Atlantic Council in the so-called „NAC + 4" format (Australia, Japan, South Korea, New Zealand) and at other political and military levels. In 2020, the focus has been on addressing the security implications of the Covid19 outbreak, but in recent years, the security situation on the Korean Peninsula and maritime security have also been discussed at NAC+4 meetings.

In December 2020, the four Asia-Pacific partners participated for the first time in the NATO foreign ministers' meeting.[17] This was a landmark event, where NATO foreign ministers discussed the changing global balance of power and China's rise with the four Asia-Pacific partners, as well as Finland, Sweden and the High Representative of the European Union, a Vice-President of the European Commission. In addition to the NAC+4 format, NATO has Individual Partnership and Cooperation Programmes with all four partner countries (New Zealand–4 June 2012; South Korea–20 September 2012; Australia–21 February 2013; Japan–6 May 2014).[18]

At the NATO Summit in Brussels in June 2021, the Allies agreed to step up dialogue and practical cooperation between NATO and existing partners, including the four Asia-Pacific Partners. The political dialogue will enable the parties to understand the security challenges (cyberspace, space, climate change) in both the Euro-Atlantic and the Asia-Pacific regions. The NATO 2030 Report confirmed and proposed the importance of consultation in the framework

---

[15] NATO 2030, p. 57–60. The two countries' exemplary relations with NATO remain in place despite their application for membership.

[16] SIPOSNÉ KECSKEMÉTHY, Klára: A NATO 2030 jelentés. Stratégiai prioritások új megközelítésben, *Honvédségi Szemle*, 2021. 4. sz. p. 3-16.; Klára Siposné Kecskeméthy: The NATO 2030 report. Strategic priorities of the Alliance, *International Conference Knowledge-based organization*, Vol. XXVII. No. 1. 2021. p. 118–124.; SZENES, Zoltán: NATO 2030. Az Észak-atlanti Szövetség újabb adaptációs kísérlete. 811-824. In Kajtár, Gábor-Sonnevend, Pál (szerk.) *A nemzetközi jog, az uniós jog és a nemzetközi kapcsolatok szerepe a 21. században. Tanulmányok Valki László tiszteletére*, Budapest: ELTE Eötvös Kiadó, 2021. 881. p.

[17] Meeting of NATO Ministers of Foreign Affairs – Brussels, 01-02 December 2020 (online event), [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_179506.htm

[18] Individual Partnership and Cooperation Programme between Australia and NATO, 29 June, 2017. [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/170629-ipcp-australia.PDF;
Individual Partnership and Cooperation Programme between New Zealand and NATO, [online]. Available on internet: https://www.nato.int/cps/en/natohq/official_texts_88720.htm;
Individal Partnership and Cooperation Programme between Japan and NATO, 26 June 2020. [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200626-ipcp-japan.pdf; NATO and the Republic of Korea sign new partnership programme, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_90101.htm, SZENES, Zoltán - SIPOSNÉ KECSKEMÉTHY, Klára: *NATO 4.0 and Hungary; 20 years of membership, 30 years of cooperation*. Budapest: Zrínyi Kiadó, 2019. 487 p.

of NATO+4, NATO-Pacific Partnership Council, the Quadrilateral Security Dialogue.

The NATO Shadow Strategic Concept document also stressed the need for the Alliance to develop deeper partnerships with the Asia-Pacific region, Australia, Japan, New Zealand, South Korea. It also included India as part of the region.[19]

At the Madrid Summit, in a clear sign of rapprochement, the Alliance invited these countries to the Summit for the first time and sat down to negotiate with Australia, New Zealand, Japan, South Korea. The strategic importance of the Asia-Pacific region is unquestionable. The presence of a rising China and Russia in the region, unresolved territorial and island disputes, nuclear-armed countries (North Korea, India, China, Pakistan) pose a serious security challenge, threat and danger. In contrast to the emphasis placed on Asia-Pacific relations at the Madrid Summit, NATO has neither the military capability nor the infrastructure to provide a concrete presence. The US security presence in the region has been a decisive factor since the WWII and remains the main ally of these countries, while France and the United Kingdom also have interests in the region.

There is a strong convergence between the objectives of the NATO Global Partnership and the ambitions and interests of the countries of the Asia-Pacific region. These countries share the core values of the Alliance, are modern democracies, their geostrategic location is well positioned and play an important role, and the future of NATO's partnership with the Asia-Pacific countries seems fundamentally secure. The network and the scope of activities have been steadily expanding over the last decade and a half. Cooperative activities focus on issues of mutual interest such as cyber defence, non-proliferation, civil preparedness and women, peace and security.

3 FINLAND AND SWEDEN NATO'S NORTHERN EUROPEAN PARTNERS – ROAD TO NATO

The NATO 2030 report already highlighted the exemplary role and contribution of Finland and Sweden to the Alliance's activities, stating that the relationship with these two countries is a model for developing partnerships in other regions.[20]

A number of security policy experts have reviewed the partnership initiatives over the past decades, always with a particular focus on the Western Five, the PfP priority countries, including Finland and Sweden. In 2004, Jeffrey Simon divided the twenty-two partner countries into groups according to their needs, interests, capabilities and geographical location, and included Finland and Sweden in the developed, Western Five.[21] Carlo Masala and Katariina Saarilouma reviewed the Alliance's partnerships, proposed a reorganisation of the partnership structure on an organisational and functional basis.[22] In 2011, NATO adopted a new more effective and flexible partnership policy, the Berlin Partnership Package.[23] In 2013, Karl-Heinz Kamp and Heidi Reisinger outlined a three-circle partnership model that allowed for broad cooperation with different countries in Europe, Asia and the Middle East, without the expectation of common policy principles and values. In their study, they put Finland and Sweden in the category of Advanced Partners.[24] In 2014, the Partnership Interoperability Initiative and the Interoperability Platform, including the Enhanced Partners group, were

[19] The TAG NATO shadow strategic concept 2022, p. 13.
[20] NATO 2030, p. 59.
[21] SIMON, Jeffrey: Partnership for Peace: Charting a Course for a New Era, March 2004. *Strategic Forum*, No. 206. pp. 1–14.
[22] MASALA, Carlo– SAARILUOMA, Katariina: Renewing NATO's Partnerships: Towards a Coherent and Efficient Framework, *Forum Paper Series*, No 1, June 2006 NATO Defense College, Rome, [online]. Available on internet: http://www.ndc.nato.int/download/publications/fp_01.pdf
[23] Active engagement in cooperative security: a more efficient and flexible partnership policy, [online]. Available on internet: http://www.nato.int/nato_static/assets/pdf/pdf_2011_04/20110415_110415-Partnership-Policy.pdf., Klára SIPOS KECSKEMÉTHY: Milestones – NATO adaptation to changing security environments, *Právo a bezpečnosť*, číslo 3. Ročník 2018. pp. 183–192. Brno
[24] KAMP, Karl-Heinz–REISINGER, Heidi: NATO's partnership after 2014: Go West!, NATO Defence College, Rome, 2013. *Research Paper* No. 92. pp. 1–8.

adopted at the Wales Summit.[25] They include the two Nordic countries, which have access to operational planning, participate in exercises and engage in regular policy consultation with the Alliance.

In 2012, Ann-Sofie Dahl described Sweden in her study as the number one operational partner and a PfP country sharing the same values as the Alliance. [26] Sweden, a non-allied country, joined the PfP in 1994, became a member of the Euro-Atlantic Cooperation Council and has developed extensive cooperation with NATO. According to Dahl, in 2012 Swedish society was divided into three groups of roughly equal size in terms of their views on NATO membership: supporters, undecideds and opponents. In her study, the author had already suggested that the two countries were likely to join NATO together because of their close historical ties and cooperation (Nordic Defence Cooperation).

Finland is in a special situation, as it shares a 1340 km border with Russia. After the end of the WWII, Finland became officially neutral, existing as a buffer zone between the Soviet Union and the Western countries. The Finnish-Soviet Treaty of Friendship, Cooperation, and Mutual Assistance (YYA Treaty – Ystävyys-, yhteistyö- ja avunantosopimus) defined the country's relations with the Soviet Union until 1991, but the country in its values was part of the Western world. Finland, like Sweden, joined the PfP in 1994, became a member of the Euro-Atlantic Cooperation Council and has also developed extensive cooperation with NATO.

Following the annexation of Crimea in 2014, both countries have further broadened and deepened their cooperation with the Alliance. However, within three months, the Russian-Ukrainian war completely changed the Finnish and Swedish public's views on the need to join NATO. Finland, together with Sweden, formally applied for NATO membership on 18 May 2022. The Madrid Summit was also an enlargement summit. The invitation of Finland and Sweden to join the Alliance was a convincing proof of the Alliance's expansion northwards for defence reasons. Turkey's veto was overridden by the trilateral Turkey-Finland-Sweden security agreement, with the strong support of the NATO Secretary General. [27] This was a clear demonstration of NATO's unity.

Following the Madrid Summit, Finland and Sweden concluded accession negotiations at NATO headquarters in Brussels on 4 July 2022, confirming their willingness and ability to assume the political, legal and military obligations and responsibilities of NATO membership. [28] On 5 July, the Allies signed the Protocol of Accession of Finland and Sweden, after which they subsequently became invited members and as such participate in NATO meetings.[29] The accession protocols must be ratified by all NATO members in accordance with national procedures. Once all Allies have ratified, the Secretary General invites Finland and Sweden to accede to the Washington Treaty, whereupon they become NATO Allies.

The final declaration of the Madrid summit confirmed NATO's open-door policy. *„Today, we have decided to invite Finland and Sweden to become members of NATO, and agreed to sign the Accession Protocols. In any accession to the Alliance, it is of vital importance that the legitimate security concerns of all Allies are properly addressed. We welcome the conclusion of the trilateral memorandum between Türkiye, Finland, and Sweden to that effect. The accession of Finland and Sweden will make them safer, NATO stronger, and the Euro-Atlantic area more secure. The security of Finland and Sweden is of direct*

---

[25] Wales Summit Declaration 2014. Para 83–85. [online]. Available on internet: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[26] DAHL, Ann-Sofie: Partner number one or NATO ally twenty-nine? Sweden and NATO post-Libya, Sept 2012, Research Paper, No. 82. p. 12. NATO Defence College, Rome. [online]. Available on internet: https://www.files.ethz.ch/isn/153549/rp_82.pdf

[27] Türkiye, Finland, and Sweden sign agreement paving the way for Finnish and Swedish NATO membership, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_197251.htm

[28] Finland and Sweden complete NATO accession talks, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_197737.htm

[29] NATO signs accession protocols for Finland and Sweden, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_197763.htm

importance to the Alliance, including during the accession process."[30]

With the two Nordic countries, the Alliance will be significantly strengthened, and the Euro-Atlantic area will be safer. The Baltic Sea will become NATO's „inland sea", changing the political and military status quo in the region. Russia have access to the Baltic Sea only through the Kaliningrad exclave. The accession of the two countries will significantly increase the common border between NATO and Russia. Previously, the common border [Norwegian-Russian 196 km, Estonian-Russian 294 km, Latvian-Russian 217 km, Lithuanian-Russian (Kaliningrad region) 227 km, Polish-Russian (Kaliningrad region) 206 km] was 1140 km long. With the accession of Finland (1340 km of the Finnish-Russian border), the common border will be 2480 km long, more than double the previous length. Finland's territory provides strategic depth for NATO and facilitates the defence of the Baltic countries. Sweden's accession will stabilise the northern border and change the geostrategic value of the Arctic and the Arctic regions.

However, the most important message of the Finnish and Swedish membership for Russia is that NATO's open-door policy remains unchanged, which could mean inviting more partner countries that share transatlantic values and strengthen the security and stability in the Euro-Atlantic area in the future.

This was a strong message in the light of the fact that on 15 December 2021, Russia handed over two draft treaties (one with USA[31] and one with NATO[32]) to the US Secretary of State for European and Eurasian Affairs. The US-Russian treaty would have guaranteed an end to NATO's eastward expansion, while the NATO agreement would have ruled out any further expansion of states of Russian interest. With regard to Ukraine, both draft treaties consistently ruled out the country's NATO membership, the military activities of NATO members on Ukrainian territory and any US-Ukrainian military cooperation.[33] Article 4 of the NATO-Russia draft asked for legally binding guarantees from NATO that they would return to NATO's 1997 borders, not deploy military forces and weapons on the territory of other European states and withdraw NATO troops from the territory of the countries that have since joined. Article 5 would have prohibited the deployment of short- and medium-range missiles in areas from which they could reach the territory of other parties. Under Article 6, all NATO member states would have committed the Alliance to refrain from further enlargement, including Ukraine and other states.

4 UKRAINE, THE STRATEGIC PARTNER

The Madrid Strategic Concept called NATO's enlargement rounds a historic success in the context of one of the Alliance's core tasks, cooperative security, and reaffirmed the open door policy of Article 10 of the Washington Treaty. It states that all European countries that share NATO's core values, accept the responsibilities and obligations of membership, and contribute to the security of the Euro-Atlantic area, have an open path to membership. The decisions of sovereign countries are not subject to interference by third parties. The Strategic Concept confirmed the declaration of the Bucharest Summit in 2008 on the accession of Ukraine and Georgia to NATO. [34]

---

[30] NATO Madrid Summit Declaration, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, [online]. Available on internet: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

[31] Treaty between The United States of America and the Russian Federation on security guarantees. [online]. Available on internet: https://augengeradeaus.net/wp-content/uploads/2021/12/20211217_Draft_RUS_USA_security_guarantees.pdf

[32] Agreement on measures to ensure the security of the Russian Federation and member states of the North Atlantic Treaty Organization. [online]. Available on internet: https://augengeradeaus.net/wp-content/uploads/2021/12/20211217_Draft_Russia_NATO_security_guarantees.pdf

[33] JÓJÁRT, Krisztián: A Moszkva által követelt biztonsági garanciákról. *Elemzések,* Stratégiai Védelmi Kutatóintézet, 2022. 1. p. 9.

[34] NATO 2022 Strategic Concept, [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

Since 2014, Ukraine's priority has been Euro-Atlantic integration, the development of a distinguished partnership with a view to achieving NATO membership. Following the illegal annexation of Crimea, NATO has reaffirmed its support to Ukraine in building a modern democratic state and strengthening its defence capabilities, through comprehensive reform of the security and defence sector, the launch of capability development programmes and the provision of financial assistance.[35] NATO members are politically united in their support for Ukraine, taking a strong stance in support of the country's sovereignty and territorial integrity within its internationally recognised borders. In the Madrid Strategic Concept, it was stated that, – after the second aggression against Ukraine – the Russian Federation is the most significant and immediate threat to the peace and stability of the Alliance and the Euro-Atlantic area.

The NATO-Ukraine partnership was a top priority among the broad themes of the Madrid Summit. Long-term financial and military assistance to Ukraine was reaffirmed under the Comprehensive Assistance Package for Ukraine agreement adopted at the Warsaw Summit in 2016. A number of programmes have been launched in recent years to support capability development and sustainable capacity building in the areas of C4, cyber defence, logistics and standardisation, medical rehabilitation, energy security, military reconversion, and disposal of ammunition and explosives. Strategic communications, the fight against hybrid warfare, security services reform and civil emergency planning are also important areas of cooperation.[36] As part of the strengthened Comprehensive Assistance Package, NATO has provided immediate assistance to war-torn Ukraine (fuel, food, medical supplies, military protective equipment and secure communications, as well as equipment against mines, drones, chemical and biological threats). NATO will provide longer-term support for the modernization of the Ukrainian Armed Forces to achieve NATO interoperability standards, as well as for the further strengthening of defence and security institutions.

CONCLUSION

The Madrid Summit was a historic event, with the most important decisions being contained in the final declaration and the strategic concept providing guidance. In Madrid, the new strategic concept of the Alliance was approved, and an agreement was reached on the introduction of a new NATO force model, which means brigade-level forward defence on the Eastern flank instead of forward presence. After Russia's actions in defiance of international law (2008 Georgia, 2014 annexation of Crimea, 2022 aggression against Ukraine) the strategic environment has changed. NATO has declared in the Madrid Strategic Concept that Russia is no longer a partner of the Alliance because of its hostile policies and actions (creation of spheres of influence, aggression, hybrid warfare, nuclear blackmail, destabilisation of countries). Nevertheless, the Alliance still maintains a dual approach, because it leaves open the possibility of continued cooperation.

Important decisions have also been taken on partner countries, with the confirmation of long-term financial and military assistance to Ukraine under the Comprehensive Assistance Package for Ukraine agreement, invitations to Finland and Sweden to join, strengthened and deepened cooperation with the Indo-Pacific partners. The invitation to Finland and Sweden to join, and the speed of the preparatory events of the enlargement round, have been very rapid. In many ways, this is a very strong message for Russia. On the one hand, NATO has reaffirmed its commitment to Article 10 of the Washington Treaty. The path to membership is open to any European partner country that shares NATO's core values, accepts the responsibilities and obligations of membership and contributes to the security of the Euro-Atlantic area. On the

[35] NATO's response to Russia's invasion of Ukraine, [online]. Available on internet: https://www.nato.int/cps/en/natohq/topics_192648.htm.

[36] Comprehensive Assistance Package for Ukraine. [online]. Available on internet: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf, NATO-Ukraine Trust Funds, [online]. Available on internet: https://www.nato.int/cps/en/natolive/topics_153288.htm.

other hand, they reiterated that the decisions of sovereign countries should not be subject to interference by third parties. Thirdly, as at every summit since 2008, Madrid reaffirmed the declaration of Ukraine and Georgia's accession to NATO. It also pledged to expand partnership with Bosnia and Herzegovina.

An important step was to strengthen and deepen cooperation with the Indo-Pacific partners. It should be noted, however, that although NATO showed extraordinary unity in Madrid, the Pacific region is not a top priority for many Central and Eastern European countries, especially those on the Eastern flank. While the Alliance's presence in the region is not made possible by its military capabilities or infrastructure, the US presence remains the primary ally for these countries. The importance of the Southern flank is unquestionable in the context of increased transnational threats and risks and the 360-degree approach of the Alliance, and therefore the partnership with the Mediterranean Dialogue countries remains important. New assistance packages have been adopted for Mauritania and Tunisia.

Finally, it was agreed that the next Summit will be held in Vilnius in 2023, an important milestone in the post-bipolar era after Prague, Riga, Bucharest and Warsaw.

BIBLIOGRAPHY

Active engagement in cooperative security: a more efficient and flexible partnership policy. [online]. Available on internet: http://www.nato.int/nato_static/assets/pdf/pdf_2011_04/20110415_110415-Partnership-Policy.pdf

Agreement on measures to ensure the security of the Russian Federation and member states of the North Atlantic Treaty Organization. [online]. Available on internet: https://augengeradeaus.net/wp-content/uploads/2021/12/20211217_Draft_Russia_NATO_security_guarantees.pdf

CSIKI VARGA, Tamás – TÁLAS Péter: Megerősített elrettentés és védelem – a NATO új stratégiai koncepciójának és madridi csúcstalálkozójának értékelése, Stratégiai Védelmi Kutatóintézet, *Elemzések*, 2022, 8. p. 1–13.

CSIKI VARGA, Tamás–ETL, Alex–TÁLAS, Péter–VARGA, Domonkos: A finn és a svéd NATO-tagság és lehetséges következményei, Stratégiai Védelmi Kutatóintézet, *Elemzések*, 2022, 7. pp. 1–11.

DAHL, Ann-Sofie: Partner number one or NATO ally twenty-nine? Sweden and NATO post-Libya, Sept 2012, *Research Paper*, No. 82. p. 12. NATO Defence College, Rome. https://www.files.ethz.ch/isn/153549/rp_82.pdf

GYARMATI, István: Egy új biztonsági rendszertelenség felé a NATO: Szép új világ. *Political Capital*, 2022. június 29. https://www.politicalcapital.hu/hireink.php?article_read=1&article_id=3025

Individual Partnership and Cooperation Programme between Australia and NATO, 29 June, 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/170629-ipcp-australia.PDF;

Individal Partnership and Cooperation Programme between Japan and NATO, 26 June 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200626-ipcp-japan.pdf;

Individual Partnership and Cooperation Programme between New Zealand and NATO https://www.nato.int/cps/en/natohq/official_texts_88720.htm;

JÓJÁRT, Krisztián: A Moszkva által követelt biztonsági garanciákról. Stratégiai Védelmi Kutatóintézet, *Elemzések*, 2022. 1. p. 9.

KAMP, Karl-Heinz–REISINGER, Heidi: NATO's partnership after 2014: Go West!, In *Research Paper,* Rome, NATO Defence College, 2013, No. 92. p. 1–8.

Madrid Summit Declaration, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022

https://www.nato.int/cps/en/natohq/official_texts_196951.htm

MASALA, Carlo– SAARILUOMA, Katariina: Renewing NATO's Partnerships: Towards a Coherent and Efficient Framework, In *Forum Paper Series*, Rome, NATO Defence College, 2006. No. 1. p. 51. [online]. Available on internet: http://www.ndc.nato.int/download/publications/fp_01.pdf

MONAGHAN, Sean- MORCOS, Pierre – WALL, Colin: What happened at the Madrid Summit, *Center for Strategic and International Studies*, 2022. [online]. Available on internet:
https://www.csis.org/analysis/what-happened-natos-madrid-summit

Madrid Summit ends with far-reaching decisions to transform NATO, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_197574.htm

NATO 2022 Strategic Concept, [online]. Available on internet:
https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO 2030: United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General", Brussels, 25 November 2020.

NATO Madrid Summit Declaration, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, [online]. Available on internet: https://www.nato.int/cps/en/natohq/topics_49594.htm

NATO New Force Model, [online]. Available on internet:
https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf

NATO and the Republic of Korea sign new partnership programme, [online]. Available on internet: https://www.nato.int/cps/en/natohq/news_90101.htm

SIMON, Jeffrey: Partnership for Peace: Charting a Course for a New Era, In *Strategic Forum*, No. 206. 2004. p. 1–14.

SIPOS KECSKEMÉTHY, Klára: Milestones – NATO adaptation to changing security environments, In *Právo a bezpečnosť*, Ročník 5. Číslo 3. 2018. p. 183–192. Brno

SIPOSNÉ KECSKEMÉTHY, Klára: A NATO 2030 jelentés. Stratégiai prioritások új megközelítésben, In *Honvédségi Szemle*, 2021. 4. sz. p. 3–16.

SIPOSNÉ KECSKEMÉTHY, Klára: The NATO 2030 report. Strategic priorities of the Alliance, In *International Conference Knowledge-based organization*, 2021. Vol. XXVII. No. 1. p. 118–124.

STEPPER, Péter: Az arányos teherviselés és alkalmazkodás kérdései a madridi csúcs előtt. Külügyi és Külgazdasági Intézet. *Elemzések*, 2022. 35. p. 1–11. [online]. Available on internet: https://kki.hu/wp-content/uploads/2022/07/KE_2022_35_ES_teherviseles_alkalmazkodas_Nato_SP_0707.pdf

SZENES, Zoltán: Elrettentés és védelem: a NATO új haderőmodellje, *Hadtudomány* . folyóirat 2022. 2.

SZENES, Zoltán - SIPOSNÉ KECSKEMÉTHY, Klára: *NATO 4.0 and Hungary; 20 years of membership, 30 years of cooperation*. Budapest: Zrínyi Kiadó, 2019. 487 p.

SZENES, Zoltán: NATO 2030. Az Észak-atlanti Szövetség újabb adaptációs kísérlete. 811–824. In Kajtár, Gábor-Sonnevend, Pál (szerk.) *A nemzetközi jog, az uniós jog és a nemzetközi kapcsolatok szerepe a 21. században. Tanulmányok Valki László tiszteletére*, Budapest: ELTE Eötvös Kiadó, 2021. 881. p.

The TAG NATO shadow strategic Concept 2022: Preserving peace, protecting people, A Report by the Alphen Group (TAG) for the Secretary General on the 2022 NATO Strategic Report, 2022. p. 1–22.

Treaty between The United States of America and the Russian Federation on security guarantees. [online]. Available on internet: https://augengeradeaus.net/wp-content/uploads/2021/12/20211217_Draft_RUS_USA_security_guarantees.pdf

WAGNER, Péter: A madridi NATO-csúcs kérdései, Külügyi és Külgazdasági Intézet, *Elemzések*, 2022. 32. p. 1–13. [online]. Available on internet: https://kki.hu/wp-content/uploads/2022/07/KKIElemzesek.KE-2022.32.pdf

Wales Summit Declaration, 2014. [online]. Available on internet: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Prof. Col. Klára SIPOSNÉ KECSKEMÉTHY, CSc
Colonel, Professor, CSc, National University of Public Service, Military Science and Officer Training Faculty, Department of Operation and Support,
E-mail: siposne.kecskemethy.klara@uni-nke.hu,
ORCID: 0000-0002-4150-7823

Alexandra SIPOS, PhD
Institute of Sociology, Centre for Social Sciences, Budapest
Junior Research Fellow
E-mail: Alexandra.Sipos@tk.hu
ORCID: 0000-0003-3855-4300

PROTECTING CITIZENS - A STRATEGIC IMPERATIVE IN A COMPLEX ENVIRONMENT OF INTERNATIONAL SECURITY

Bożena KONECKA-SZYDEŁKO, Dorota WŁODYKA-TYCZYŃSKA

ABSTRACT

Along with the development of mankind, new types of armed conflicts arise, and technological progress enables the creation of modern means of combat. Unfortunately, one feature of war has never changed - it has always been a threat to the civilian population, who suffer the most because of it. The UN estimates that 100 civilians die in conflicts every day.

In Ukraine, the armed forces of the Russian Federation are shelling civilian infrastructure, threatening nuclear facilities and refusing civilians to evacuate safely from conflict zones. If the armed forces rest on the foundations of international humanitarian law (law of armed conflict) and implement strong safeguards in their day-to-day operations, they can limit civil damage. The better the civilian population is protected, the greater its resilience and support for stability and lasting peace.

Keywords: humanitarian law, armed conflict, civilian population.

INTRODUCTION

International humanitarian law of armed conflicts is a term used to describe a branch of public international law that relates to the main norms and standards of military operations (Milik, 2017, p. 96). The protection of civilians in the broad sense is one of the most important and most difficult goals set for international humanitarian law of armed conflicts. The law of war [lat. ius in bello] (Mojsiewicz, 1998), by regulating the rules and giving guidelines for the conduct of armed struggles and clashes (Barcik, 2019), it also tries to counteract victimization of civilians.

The civilian population, as it is particularly threatened by various negative effects of military operations, is subject to exceptionally strong legal protection in the norms of international humanitarian law. A particularly glaring example of the failure to respect public international law and the failure to protect civilians was the period of World War II. Especially Germany (Góralczyk, Sawicki, 2017, p. 433) and Japan (Stawarz, 2020) at that time committed incredibly serious crimes against the civilian population of the occupied territories. as part of a total war.

The 2010 diagnosis that "there is peace in the Euro-Atlantic area and the threat of a conventional attack on NATO territory is low" no longer applies. Russia's illegal annexation of Crimea in 2014, a long hybrid war against Ukraine, and finally a full-scale attack in February 2022 made the specter of a conventional war and a potential confrontation of great powers return to European politics (https://www.nato.int/docu/review/pl/articles/2022/06/17).

Hybrid threats, energy crises, rising food prices and the economic and social impact of a pandemic further complicate the already complex security environment. In asymmetric, non-international conflicts, e.g. the conflict in Darfur, which is currently one of the largest humanitarian crises in the world (Wiatr, 2020), it is estimated that about 80-90% of conflict victims are civilians today (Lubiński, 2014).

Due to the ongoing Russian invasion of Ukraine, millions of people have fled from Ukraine, and many others became internally displaced persons. Many of them have been

illegally killed, others struggle with a lack of access to critical infrastructure as well with sexual violence. During the first 100 days (https://www.ohchr.org/en/news/2022/06/ukraine) of intense hostilities in Ukraine, when the Russian Federation passed (https://civiliansinconflict.org/wp-content/uploads / 2022/03 /) from general fire to targeted attacks on civilians and civil infrastructure, 4,339 civilians were killed and 5,246 injured; these figures probably do not include the significantly greater number of unconfirmed civilian casualties. After 100 days of fighting, almost 5 million Ukrainians have happened become (https://data.unhcr.org/en/situations/ukraine) refugees in Europe, and over 7 million have become (https://www.unhcr.org/ua/en/internally-displaced-persons) internally displaced persons. In Ukraine, the armed forces of the Russian Federation reportedly fired on civilian infrastructure, threatened nuclear facilities, and refused civilians to safely evacuate conflict zones.

In most wars, the civilian pays the highest price. The United Nations estimates (https://www.un.org/sustainabledevelopment) that every day 100 civilians die in conflicts. Between 2001 and 2021, 387,000 civilians are thought to have lost their lives as a direct result of the aftermath of the aftermath of September 11, 2001, and many more suffered indirect consequences of the hostilities, such as the destruction of critical infrastructure.

Protecting civilians is a key aspect of warfare and an ethical and strategic imperative in all types of conflict, from hybrid warfare to counterinsurgency and large-scale military operations, where the adversary may employ tactics to harm civilians. Nearly two decades of military operations and assistance to security forces in Afghanistan and the Middle East have only confirmed that harm reduction to the civilian population is a prerequisite for the success of military operations and security partnerships.

The better the civilian population is protected, the greater its resilience and support for stability and lasting peace.

If the armed forces rest on the foundations of international humanitarian law (the law of armed conflict) and implement strong safeguards in their day-to-day operations, they can limit the civil damage resulting from their own operations and can protect civilians from the adversary's actions. During the International Security Assistance Force (ISAF) mission in Afghanistan, the Allies adopted innovative solutions to mitigate the damage caused to the civilian population. NATO adopted a policy of protecting civilians during the Warsaw summit in 2016, followed by the military concept (2018) (https://www.nato.int/cps/en/natohq/official_texts 2022) and Implementation Manual (2020) (https://shape.nato.int/news-archive/2021), and conducted a series of exercises to test NATO forces.

However, since this policy was mainly based on lessons learned in the field of counterinsurgency, it is not clear that its relevance to any possible Article 5 operation has been well understood or has found operational application.

Due to the increasing risk and the acute helplessness of civilians in the face of conflicts inside and outside NATO, NATO now has a unique opportunity to emphasize its political commitment to protecting civilians and to issue a strong mandate and guidelines for its implementation, which will lead to prioritization of protection. in NATO and national institutions (MacLachlan, 2022). This should lead to a security priority given to Allies and Alliance institutions in three key dimensions:

- As a value-driven imperative for the Alliance to protect NATO members and their citizens;
- As an indispensable element of an effective strategy, enabling armed forces to support political goals while shielding civilians from the worst consequences of the conflict; and
- A key element contributing to a country's resilience.

However, a political commitment should only be the beginning of the road and a mandate for its implementation. On the practical side, there are several key actions that NATO forces can take to prepare for potential hostilities at home (MacLachlan, 2022). Processes also arise that can help translate political commitment into military procedures and resources. NATO has the opportunity to signal the need for their implementation.

1 SOURCES OF PROTECTION FOR THE CIVILIAN POPULATION

The sources of international humanitarian law regulating the most important issues related to the protection of civilians in an armed conflict are, first of all, the Fourth Geneva Convention of August 12, 1949 for the Protection of Civilians in War (hereinafter: IV KG, Journal of Laws of 1956, No. 38, item 171), Protocol I to the Geneva Conventions on the protection of victims of international armed conflicts (hereinafter: I PD, Journal of Laws of 1992, No. 41, item 175) and Protocol II to the Geneva Conventions on protection of victims of non-international armed conflicts (hereinafter: II PD, Journal of Laws of 1992, No. 41, item 175). Moreover, positive international law (treaty) complements the rules, principles and norms of customary law developed over time, e.g. the principle of distinction, which is also the principle of positive law (Łubiński, 2014, p. 210).

Regional and national legal instruments which, as a subsidiary, counteract negative phenomena directed against civilians, which form part of the refugee law, are also of great importance in the local protection of the civilian population against military actions (e.g. the Convention on specific aspects of the problem of refugees in Africa of September 10, 1969 (the Convention on specific aspects of the problem of refugees in Africa). ..., 2020) or the Cartagena Declaration of November 22, 1984 (Declaration ..., 2020).

One should also not overlook the rich, thematic jurisprudence of international judicial bodies, such as the International Criminal Tribunal for the former Yugoslavia ICTY (UN Information Center ..., 2020). A legal definition of a civilian person and civilian population can be found in Art. 50 of the 1st Additional Protocol to the Geneva Conventions in Chapter II, Part I, Part IV, entitled "Civilians and the civilian population".

These terms are described by means of negative premises and references to other definitions and regulations. “The advantage of a negative definition is that it guarantees a disjointed division - a given person can be either a combatant or a civilian; a given person can never belong to both categories at the same time, nor belong to either of them” (Łubiński, 2014, p. 211).

Any person not belonging to any of the defined categories is considered to be civil in art. 4 A item 1), item 2), item 3) and item 6) of the 3rd Geneva Convention (hereinafter: 3rd KG) and in art. 43 Of the 1st Additional Protocol. Thus, taking into account the above-mentioned regulations, a person who: “is a member of the armed forces, parties to the conflict or a member of the militia and volunteer units that are part of these armed forces cannot be considered a civilian (point 1); is a member of other militias and other voluntary units, including a member of the organized resistance movement (point 2); is a member of the armed forces which define themselves as being subordinate to an unrecognized government or authority (item 3); belongs to the mass movement (people spontaneously grabbing their weapons in the face of an approaching enemy, the so-called levee en masse (point 6) ”(Łubiński, 2014, p. 211). Article 43 I of the PD contains the definition of the armed forces.

Undoubtedly, the armed forces consist of all armed and organized forces, groups and units that are under the command of a party to a conflict responsible for the conduct of its subordinates, even if that party is represented by a government or authority not recognized by the other party. Such armed forces should have a subsystem of internal discipline which ensures respect for the rules of international law applicable in armed conflicts. A party to a conflict that

integrates a paramilitary organization or an armed public order service into its armed forces should notify other parties to the conflict about it (Art. 43 I of the PD). Importantly, Art. 50 point 1 of Additional Protocol I introduces the presumption of the status of a civilian. According to this legal structure, if it is not known whether a given person is definitely a civilian, then their civil nature should be presumed. This understanding of having the status of a civilian was also confirmed by the International Criminal Tribunal for the former Yugoslavia (ICTY), although it noted that this status should be interpreted as broadly as possible (Ruling of the Appellate Chamber ..., 2020). I Additional Protocol in Art. 50 points 2 and 3 presents in a simple manner and a clear definition of the civilian population.

According to the aforementioned regulations, the meaning of civilians includes: all civilians living in a given area - in the narrower sense (point 2), civilians of a given state – in a broad sense, and the presence of individuals among this group (e.g. enemy combatants trying to hide) civilians who do not meet the term does not deprive them of their civil nature or protected humanitarian law (point 3). This is also confirmed by the extensive jurisprudence of the ICTY (Szpak, 2009, pp. 62-68). Therefore, the civilian population is protected in its entirety, on the basis of equality, regardless of race, religion, nationality or political beliefs, art. 75 I PD, (Góralczyk, Sawicki, 2017, p. 432). Moreover, civilians, as protected by the norms of humanitarian law, may demand respect in all circumstances for their customs and customs, religious practices and worship, dignity, honor and veneration, art. 27 IV KG (Góralczyk, Sawicki, 2017, p. 432). Pregnant women and children are particularly protected (eg Articles 76–78 I PD). The parties to the conflict should therefore distinguish between the civilian population and combatants and therefore direct their operations only against military targets (Art. 51 (1) and (2) of the PD), and not against civilians and objects (Bierzanek, 2004).

2 THE SITUATION OF THE CIVILIAN POPULATION IN THE FACE OF MILITARY ACTIONS

The issue of protection of the civilian population can be considered on two basic levels: military operations and staying under the power of the party to the conflict, e.g. as a result of the war occupation (Łubiński, 2014, p. 2011). As a result of the activity of the parties to the conflict, international humanitarian law finds its application, counteracting the negative effects of these activities. "In the course of military operations, the fighting parties are primarily obliged to observe the basic principles of humanitarian law - the principles of humanitarianism, proportionality and differentiation" (Łubiński, 2014, p. 2011).

The principle of humanitarianism prohibits causing unnecessary suffering (eg in Art. 54 I PD). On the other hand, the principle of proportionality defines the need to maintain a balance between military necessity and the needs of humanitarianism (eg in Art. 57 I PD). The principle of distinction, especially emphasized in the 1st Additional Protocol (e.g. in Art. 52 of I PD), requires that each time a mental operation should be made to distinguish between military and non-military objects.

The targets of attacks cannot be against the civilian population as such, or against civilians (Art. 51 (2) sentence 1 I PD). Acts and threats of violence, the main purpose of which is to intimidate the civilian population, are prohibited (art. 51 item 2 sentence 2 I PD). Attacks without distinction are also prohibited (Art. 51 (4) I PD): attacks that are not directed against a specific military target (a); attacks that use methods and means of combat that cannot be limited to a specific military purpose (b); attacks where methods are used and measures of combat, the effects of which cannot be limited and, consequently, in each of these cases may be indistinguishably between military and non-military objectives (c); attacks in the form of bombing, regardless of the methods and means used, which treat as a single military target a certain number of clearly outlined military targets and distinctive, located in a city, village or

other zone with a similar concentration of civilians or civilian properties (Article 51 (5) (a) of the PD); attacks which may be expected to also cause loss of human life to the civilian population, injury to civilians, damage to civilian property, or a combination of these losses and damages if they are excessive compared to the specific expectation expected and a direct military benefit (Article 51 (5) (b) of the PD).

The issue of the protection of bystanders is also important for the armed forces themselves involved in the conflict. Parties to the conflict are required to take special precautions to avoid civilian casualties. "Commanders planning or deciding to launch an attack should do everything possible to check and ensure that the target of the attack is not civilians or civilian goods" [Art. 57 point 2 lit. a and art. 87 I PD], (Łubiński, 2014, p. 2012). The attack should be abandoned or discontinued when it is found that its purpose is not of a military nature or benefits from special protection, or that it can be expected to cause unintended loss of human life to the civilian population, injury to civilians or damage to property civil nature (Article 57 (2) (b) I PD). When selecting the means and methods of attack, the commander must take all practically possible precautions to avoid, or at least reduce to a minimum, unintended losses in human life among the civilian population (Article 57 (2) (a) of the PD). In the event that attacks may endanger the civilian population, a timely warning should be issued, unless circumstances do not allow it (Art. 57 (2) (c) of the PD). If it is possible to choose between several military objectives for the purpose of achieving the same military benefit, the target whose attack poses the least danger to civilians or civilian goods (Article 57 (3) I PD) should be selected. Any breach of these prohibitions shall not release the parties to the conflict from their legal obligations in relation to the civilian population and to civilians (art. 57 point 5 I PD). Therefore, the civilian population and civilians enjoy general protection against dangers resulting from military operations (Article 57, point 4 and Article 51, point 1 of the PD). It is forbidden to use starvation against civilians as a method of warfare (art. 54 point 1 of the PD). Moreover, attacks aimed at reprisals against the civilian population or against civilians are prohibited (Art. 51 (6) I PD). Finally, the presence or movement of the civilian population should not be used to protect certain points or zones, in particular in an attempt to protect military targets from attack, or to mask, facilitate or obstruct military operations.

The parties to the conflict should not direct the civilian movement in such a way that it constitutes an attempt to cover military operations (art. 51, point 7 I of the PD). Thus, the civilian population cannot be used as the so-called living shields (Milik, 2017, p. 96). Also robbery, collective punishments, robbery and taking civilians hostage are strictly prohibited, Art. 75 point 2 I PD (Góralczyk, Sawicki, 2017, p. 433). It is also prohibited to place military targets inside or adjacent to densely populated areas.

The parties to the conflict are obliged to keep civilians, civilians and civilian goods under their control away from military targets (Art. 58 I PD). Civil goods should also not be the target of attacks (art. 52 point 1 sentence 1 I PD). They cannot be the target of reprisals (art. 52 point 1 sentence 1 and art. 54 point 4 I PD). According to the negative definition of these goods, contained in Art. 52 point 1 sentence 2 of the 1st Additional Protocol, all non-military goods are civilian goods. The aforementioned legal act presumes that, in case of doubt, it is presumed that goods normally intended for civil use, such as a place of worship, a house, other living quarters or a school, are not used to make a real contribution to a military action (Art. 52 point 3 I PD).

Attacks should be strictly limited to military purposes (art. 52 point 2 sentence 1 I PD). On the other hand, military purposes are only those goods and objects which, due to their nature, location, purpose or use, make a significant contribution to military activity and whose total or partial destruction, seizure or neutralization gives a specific benefit in a given situation (Art. 2 sentence 2 I PD). It is forbidden to attack, take or destroy goods necessary for the survival of the civilian population in order to prevent the opposing party from using of them (art. 54 point

2 I of the PD), unless the goods are used only for the maintenance of members of the armed forces or for other purposes, but for direct support of a military operation (art. 54 point 3 I of the PD). Under no circumstances, however, shall measures be taken against these goods, which could be expected to leave the civilian population with so little food or water that it would be exposed to starvation or forced to move (Article 54 (3) (b) of the PD).

3. CIVILIAN POPULATION UNDER THE AUTHORITY OF THE PARTIES TO THE CONFLICT

The situation of the civilian population under the authority of the parties to the conflict is mainly related to the state of occupation. "A war occupation is a temporary seizure by the armed forces of a militant state of part or all of the enemy's territory and the establishment of actual power there" (Góralczyk, Sawicki, 2017, p. 433). Therefore, it consists mainly in the actual management and possession of the occupied area from the moment of the entry of foreign troops (National Defense University ..., 2020). From the perspective of international law, this is obviously a temporary situation. "During the occupation, humanitarian law grants civilians a number of rights, at the same time imposing on the military administration of occupation an obligation to respect these rights", Art. 2 IV KG (Łubiński, 2014, p. 212).

The occupying power should provide, to the greatest extent possible, and without any disadvantage, the supply of clothing, bedding, temporary accommodation and other supplies essential for the survival of the civilian population of the occupied territory, as well as articles necessary for religious worship (Art. 69 point 1 I of AP and art. 55 IV of the KG). The supreme rights and guarantees for civilians in the occupied areas are contained in Art. 75 of Additional Protocol I (although the provision itself has a much wider application and does not only apply to the state of occupation). They include issues related to the protection of health, life and dignity and freedom. These persons are protected regardless of race, color, sex, language, religion or belief, political or other opinion, national or social origin, property, birth or other characteristics, or on account of any other similar criteria (point 1 sentence 1). Each party should respect their dignity, beliefs and religious practices (point 1 sentence 2). In addition, the following acts against this category of persons are prohibited (point 2): attacks on life, health or physical or mental balance (in particular murder, torture in all its forms, physical and mental, corporal punishment and mutilation); outrages on personal dignity, in particular humiliating and degrading treatment, forced prostitution and all forms of indecency attacks; hostage-taking; collective punishments; threats to commit any of the above-mentioned acts.

As regards the protection of property, the civilian population retains the right to respect private, public, collective and cooperative property, however, this protection may be limited when it comes to absolute military necessity resulting from military operations, art. 53 IV KG (Łubiński, 2014, p. 213). It is also forbidden to force the population of the occupied territories to serve in the armed forces of the occupant, auxiliary forces (art. 51 sentence 1 IV KG); promoting recruitment to volunteer forces (art. 51 sentence 2 IV KG); deportation of people from the occupied areas and resettlement of the population of the occupying party to the occupied areas (Art. 49 IV KG). Temporary evacuation of civilians can be used exceptionally, but only for their safety. Civilians also have the right to send and receive family messages and to search for members of their families dispersed by the war (Art. 74 I PD and Art. 25 IV KG).

These persons are also entitled to receive postal items containing medicines, items for religious practice, as well as food and clothing (Art. 69 I PD). Citizens of the occupied state may only be compelled to perform forced labor which is normally necessary for the provision of food, housing, clothing, transport and health and which are not directly related to with the conduct of hostilities (art. 51 IV KG). In the areas occupied by the militant parties, three legal orders are temporarily in force: the domestic law of the occupied state (Art. 64 IV KG), the law

imposed by the occupant (Art. 64 and 65 IV KG) and international law (Góralczyk, Sawicki, 2017, p. 433).

The national law is still in force despite the occupation, as the occupier only manages the occupied area (Antonowicz, 2015, p. 261). Due to the complexity of the actual situation, the occupant obtains the right to issue its own norms modifying the existing legal system. The occupier should, however, as far as possible refrain from changing local legislation unless absolutely necessary. The same principle may still operate local courts in the occupied territories, as long as it does not endanger the security of the occupation forces (Articles 54, 64 and 66 IV KG).

On the other hand, absolutely binding international law is irrevocable in the form of customary standards, currently codified in the Fourth Geneva Convention of 1949. This law prohibits, in particular, the imposition of collective penalties, violation of the principle of *nullum crimen* sine *lege* or the principle of *lex retro non agit* in criminal trials, the destruction of private, state, cooperative property, property of social organizations and its confiscation (with the exception of the spoils of war, but only in relation to movable property). Except in cases of detention or imprisonment for a crime, the detained person should be released as soon as possible, and in any case when the circumstances justifying arrest, imprisonment or internment have ceased to exist (art. 75 point 3 sentence 2 I PD). Every accused must have the right to be heard in his presence.

Criminal proceedings should respect all guarantees of a proper trial (art. 75 point 4 I PD and art. 71-78 IV KG), such as: the right to defense, including the right to with the help of a qualified lawyer; the right to prove one's point, including by presenting evidence, even in the form of calling witnesses; the right to use possible remedies. Punishment for a crime should be made only on the basis of personal criminal liability, and the accused should be able to request that the sentence be pronounced publicly. Of course, it is absolutely forbidden to force an explanation or admission of guilt. “In the event of a breach of criminal law, the occupying state may hand over the accused to its military courts located in the occupied territory. […]. In the case of acts of a lower risk, a penalty of internment or imprisonment should be imposed. On the other hand, the death penalty can be imposed only in the case of acts defined as espionage, acts of severe sabotage or an intentional crime that resulted in the death of at least one person ”(Łubieński, 2014, pp. 214-215).

However, the death penalty may not be imposed and executed against a convicted person who was under 18 years of age at the time of committing the offense (Art. 77 (5) I PD and Art. 68 IV KG). Convicted persons should serve a valid sentence of imprisonment, if possible, in the occupied country, and after the occupation, they should be handed over to the judiciary and the services of the occupied state (Articles 76 and 77 IV KG). Humanitarian law grants women and children exceptional protection in the course of an armed conflict (Articles 76–78 of I PD, eg Articles 14 and 24 of the IV KG). In fact, these persons should be included in the group of civilians under special protection (Art. 16 IV KG). Among them, special treatment is granted to pregnant women, obstetricians and mothers of young children. Thus, women who find themselves in an area covered by an armed conflict should enjoy special respect and protection, especially against rape, forced prostitution and any other form of attack on morality (Art. 76 (1) I PD and Art. 27 IV KG). Children as persons under special protection may also benefit from special respect (Art. 77 (1) of the PD). They should be protected against any attacks on morality. The parties to the conflict have a duty to provide them with the care and assistance they need due to their age (but also for any other reason), and to take all practicable steps to prevent children under the age of 15 from participating directly in hostilities (Art. 2 sentence 1 I PD).

4 PROTECTION OF THE CIVILIAN POPULATION IN NON-INTERNATIONAL ARMED CONFLICTS

International humanitarian law also applies to the protection of civilians in armed conflicts of a non-international nature. However, unlike in conflicts between states, these issues are regulated primarily by the Second Additional Protocol to the Geneva Conventions and the legal regime resulting from Art. 3 common to all Geneva Conventions (Marcinko, 2019, p. 97).

The civilian population and civilians enjoy general protection against dangers resulting from military operations (art. 13, point 1, PD). Moreover, the civilian population as such cannot be targeted by attacks and should also be treated humanely at all times (Article 3, common to the four Geneva Conventions). Acts or threats of violence, the main purpose of which is to intimidate this population, are prohibited (Article 13 (2) of the Second PD). Also, the use of starvation as a means of fighting against them is prohibited. For this reason, it is also forbidden to attack or make unusable goods necessary for the survival of the civilian population, e.g. food supplies, crops, cattle or drinking water facilities (Art. 14 II PD). The displacement of this community by a party to the conflict for reasons related to the conflict is prohibited, unless its safety or decisive military considerations so require (art. 17 point 1 of II PD). In addition to ordinary civilian goods, in the course of a non-international armed conflict, the protection of areas of special humanitarian law, such as non-defended localities, sanitary zones and localities, and demilitarized zones, was also covered - on a similar basis as in the case of an international conflict (Marcinko, 2019, p. 447). Finally, it should be mentioned that civilians who take direct part in hostilities lose their protection for the duration of this participation (Art. 13 (3) II AP). "The effect of this participation is only the loss of protection, and the person taking part in the hostilities does not lose the status of a civilian. [...] However, direct participation in hostilities may be the basis for the application of criminal sanctions, if such a possibility is provided for in the criminal legislation of a given state" (Marcinko, 2019, p. 371).

5. CURRENT CONCEPTS OF NATO'S NORTH ATLANTIC ALLIANCE IN THE FIELD OF PROTECTION OF CIVILIANS

NATO's planning must take into account four key trends that are likely to shape civilian protection in the decades to come.

First of all, to provide effective protection and mitigate any resulting damage through their own actions, NATO and the governments of its member states **must engage in dialogue with civilians in a routine and specific way** (Kepe & Osburg, 2017). This should include building capacity, procedures, communication channels and developing proactive habits to engage with communities and civil society in hostilities - all of these elements can help armed forces understand the operational environment and the impact of military presence and operations on the civilian population, and help better predict their behavior in a conflict. Community engagement - carried out out of sight where such links could pose a threat to the civilian population - is also essential if the armed forces hope to gain and maintain the support of the civilian population in the area of operations. In peacetime, non-NATO actors, including civilian authorities and civil society organizations, can be valuable partners in ongoing dialogue, planning and exercises, especially for NATO institutions and allies likely to be most affected by the changing security situation, including the Baltic States, Poland and Allies contributing to an Enhanced Forward Presence.

Second, the Alliance **must make the most of the processes at its disposal** - the NATO Defense Planning Process (NDPP), Graded Response Plans (GRP), and an extensive exercise structure - to ensure that the capabilities needed to protect civilians (intelligence assets, military

training, crisis management) are taken as seriously as those enabling warfare, and solid standards have been adopted across the Alliance.

These processes can help promote **the uptake of new good conservation practices**, including Civilian Harm Tracking (CHT) units developed and tested by ISAF in Afghanistan (Civilian Harm Tracking, 2014, pp. 20-24). Built into planning, adequately resourced and tested during exercise, CHT units can monitor and analyze civil damage incidents and recommend tactical and operational modifications to reduce, prevent and mitigate incidents involving civilians. States should also consider establishing procedures to respond to damage caused to civilians - from medical assistance to remedial mechanisms - which can not only help mitigate the damage but also build better civil-military relationships.

Third, Allies will need **to develop and provide information on approaches to conflicts in which civilians and civilian infrastructure may be intentionally attacked**; experiences from Syria and Ukraine suggest that this is a likely scenario. This will require NATO forces to prepare for situations where protecting civilians from the actions of others becomes a priority, as well as the ability to shape military operations, gather intelligence, and cooperate. with non-NATO actors in a manner that enables early warning and efficient civil-military coordination (MacLachlan, 2022).

Fourth, the increased importance of preparedness for Article 5 operations does not mean that Allies should lose sight of the support of the security forces, **including in the context of the fight against terrorism**. NATO's cooperative security partnerships have already provided (Godefroy, Baran 2021) opportunities to promote the adoption of robust security standards among Partner countries. Recent experiences and innovative solutions implemented by partners, as well as lessons from the war in Ukraine - both in terms of types of civil damage and response to them - must be included in NATO's partnership packages to benefit the preparedness of others (MacLachlan, 2022).

The revival of intense military operations in the politics of great powers carries the risk of conflicts spilling over and escalating. Conflicts involving great powers are no longer a distant memory - they have become rather risks to be faced. In preparation for strengthening defense on the eastern flank, NATO members will have to consider civil protection policy as a key element of their strategy and force structure shaping. They will have to take into account the attitudes of the Baltic states regarding "total defense" (Kepe & Osburg, 2017) and their possible implications for the protection of civilians, take into account the large-scale movement of people and apply knowledge and practices in the field of civil protection acquired on their own territory. during expeditionary operations.

NATO adopted a civil protection policy in 2016 at the Alliance summit in Warsaw, then adopted the Military Concept (2018) and Implementation Manual (2020) and conducted a series of exercises to test NATO forces. Pictured: NATO is trying to protect civilians in Afghanistan.

In the event of an escalation of conflicts, the confrontation of great powers may be aggravated by urban struggles: the war in Ukraine shows that the strategic value of cities and their role in running the country's life could shift fighting to the streets. Complex terrain, including suburban areas, difficulties in distinguishing civilians from military opponents, the proximity of military targets to civilian infrastructure, difficulties in maintaining effective command and control, and short reaction times make cities difficult territory for the military. For civilians, the damage (Wars in pitie ..., 2022) caused by the use of explosive weapons in populated areas and the repeated echoing effects of the destruction of infrastructure - from hospitals to power plants - can make cities impossible to live in. This is especially true when the enemy conducts mass attacks or deliberately hits civilians - in Ukraine, forces of the Russian Federation fired at civilian facilities, endangered nuclear facilities, and refused to safely leave the conflict areas for civilians.

Below the threshold of full-scale kinetic operations, **hybrid warfare** has become an integral part of the arsenal of great powers (Bilal, 2021). Used to spread distrust and create an environment where it is more difficult to end conflict, it often contains a significant component of information warfare as civilian casualties can be manipulated, militarized and used to dominate the information space. Initial research into the war in Ukraine indicates that disinformation tactics can cause physical harm as it shapes reactions and individual decisions.

Finally, **civil wars** are likely to remain the most dominant form of conflict in the world. Brutal actions by security forces and non-state actors can lead to cyclical acts of violence against the civilian population, prolong conflicts and delay development for decades. Frequent involvement of external actors - be it through security assistance or the use of private military companies (PMCs) that carry out military and related tasks. with security in conditions of conflict and instability - can complicate the battlefield and make it difficult to determine responsibility (Kubiak, 2022). The activities of military companies may increase the risk to the civilian population. Due to the presence of many entities chains of command and control, it also makes it difficult to bring anyone to justice for abuses in hostilities.

CONCLUSION

International humanitarian law of armed conflicts provides a well-established legal framework for the protection of civilians and civilians in an armed conflict. The Geneva Conventions and the Additional Protocols play a special role in this respect. However, both treaty law and customary law are complementary and complementary elements of the system of public international law. Although a large part of humanitarian law norms are mandatory norms, it should be noted that there is currently no fully effective system of responding to violations and enforcing these rules and regulations.

Certain subsidiary assistance is, of course, the criminal legislation of individual countries and international criminal law for the prosecution of the perpetrators of the most serious crimes. However, the protection of civilians in armed conflicts is not only about subsequent criminal reactions, but also about the humanitarian aid provided by numerous NGOs. It can therefore be concluded that the protection of civilians during an armed conflict is based on many levels, including civil defense or the issue of assistance to refugees and internally displaced persons.

It is also important to disseminate knowledge about international humanitarian law among members of the armed forces around the world. Selected aspects of the protection of civilians clearly show that in the current - international and national - legal systems there are sufficient legal and theoretical foundations for the effectiveness of this protection, and the only aspect requiring thorough improvement is the practice of implementing these regulations and raising awareness of their validity.

Given the unpredictability of the security situation in Europe, it is imperative that NATO and its individual members fine-tune their values-based commitment to protecting civilians through political guidance, military doctrine, standard operating procedures and training. The end goal is to enable NATO members as well as the forces put at the disposal of the Alliance - from the NATO Response Force to the Multinational Corps Northeast and elements of an Enhanced Forward Presence - to mitigate the damage caused by their own operations and to protect civilians from the actions of others.

While the Concept is the starting point and much of the security work will be done in NATO institutions and national governments, once adopted, it will be key to fostering consensus, identifying relevant trends, and determining priorities and direction for further work.

BIBLIOGRAPHY

Additional Protocols to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts (Protocol I) and to the Protection of Victims of Non-International Armed Conflicts (Protocol II) of 8 June 1977 (*Journal of Law*s No.of 1992, No. 41, item 175).

ANTONOWICZ, L. 2015. *A textbook of international law*, Warsaw, p. 261, ISBN: 978-83-264-9255-6.

BARCIK, J. 2019. Ius in bello, [in:] Barcik J., Srogosz T., *Public international law*, Warsaw , p. 689, ISBN 978-83-255-9597-5.

BIERZANEK, R.2004. The law of armed conflicts, [in:] R. Bierzanek R., Symonides J., *Public international law*, Warsaw , p. 409, ISBN: 978-83-7334-294-1.

BILAL, A. 2021. *Hybrid war - new threats, complexity and "trust" as an antidote*, 30.11.2021 [online]. https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa- new-zagrozenia-zlozonosc-i-trust-as-antidotum / index.html (access: (20/09/2022).

Civilian Harm Tracking: *Analysis of ISAF Efforts in Afghanistan, 2014*, pp. 20-22, https://civiliansinconflict.org/wp-content/uploads/2017/09/ISAF_Civilian_Harm_Tracking.pdf (accessed on September 21, 2022).

Convention on specific aspects of the problem of refugees in Africa of 10 September 1969 [accessed 10.10.2020].

Conventions for the protection of war victims of August 12, 1949 (*Journal of Laws* of 1956, No. 38, item 171), http://libr.sejm.gov.pl/tek01/txt/inne/ 1949-4.html, (access: 20/09/2022).

GODEFROY, B., BARAN L., MAMUTOV, S. 2021. Building bridges, reinforcing protection: how NATO's protection of civilians framework influenced Ukraine's approach, 2021, [online] https://www.stimson.org/wp-content/uploads/2021 /07/ProtectingCivilians_FinalProof3348.pdf (accessed: 20/09/2022).

GÓRALCZYK, W., SAWICKI, S,2017. *An outline of public international law*, Warsaw , pp. 432-433. ISBN: 978-83-8223-147-2, https://www.nato.int/cps/en/natohq/official_texts_133945.htm (accessed: 20/09/2022).

ICTY Appeals Chamber ruling in the case of Milan Martić of 8 October 2008, IT-95-11-A, https://www.amnesty.org/en/wp-content/uploads/2021/05/POL300022014POLISH. pdf (access: 15/10/2020).

https://www.nato.int/docu/review/pl/articles/2022/06/17/ochrona-ludnosci-cywilnej-staly-punkt-odniesienia-w-zmieniajacym-sie-srodowisku-bezpieczenstwa/index.html (access: 20/09/2022).

https://www.ohchr.org/en/news/2022/06/ukraine-civilian-casualty-update-10-june-2022 (access: 20/09/2022).

https://civiliansinconflict.org/wp-content/uploads/2022/03/Emerging-Patterns-of-Civilian-Harm-in-Ukraine_Final.pdf (access: 20/09/2022).

https://data.unhcr.org/en/situations/ukraine (access: 20/09/2022).

https://www.unhcr.org/ua/en/internally-displaced-persons (accessed: 20/09/2022).

https://www.un.org/sustainabledevelopment/wp-content/uploads/2020/07/E_infographics_16.pdf (access: 20/09/2022).

https://shape.nato.int/news-archive/2021/the-protection-of-civilians-allied-command-operations-handbook#:~:text=The%20handbook%20is%20to%20tool,long%2Dterm%20security% 20and% 20stability (access: 20/09/2022).

KEPE, M, OSBURG, J. 2017. Total Defense: How the Baltic States Are Integrating Citizenry Into Their National Security Strategies, 09/24/2017, [online] https://smallwarsjournal.com/jrnl/art/total-defense-how- the-baltic-states-are-integrating-citizenry-into-their-national-security-(accessed: 20/09/2022).

KUBIAK, K. 2022. War as a service. How do private military companies destroy democracy? Weekly Civic Affairs, No. 117 / (13), 2022, [online] https://instytutsprawobywatelskich.pl/wojna-jako-usluga-jak-prywatne-firmy-wojskowe-niszcza-demokracji/ (20/09/2022).

ŁUBIŃSKI, P. 2014. Protection of the civilian population. Protection of refugees, [in:] Falkowski Z, Marcinko M. (ed.), *International humanitarian law of armed conflicts*, Warsaw, pp. 209-215, ISBN 978-83-63755-37-9.

MACLACHLAN, K. 2022. Protection of civilians - a constant point of reference in a changing security environment, 17/06/2022, [online] https://www.nato.int/docu/review/pl/articles/2022/06/17/ochrona-ludnosci- civil-constant-reference-point-in-changing-sie-srodowisku-Bezpieczenstwa / index.html, (accessed: 20/09/2022).

MARCINKO, M. 2019. The normative paradigm of military action in a non-international armed conflict, Wrocław, pp. 97,447,371, ISBN: 9788366248014.

MILIK, P. 2017. Fundamentals of international humanitarian law of armed conflicts, [in:] Kitler W., Nowak D., Stepnowska M. (eds.), *Military Law*, Warsaw, p. 96, ISBN: 978-83-8124 -039-0.

MOJSIEWICZ, C. (ed.). 1998. Lexicon of contemporary international political relations, Wroclaw, TIN: T00094663.

National Defence Academy, Dictionary of terms in the field of national security, Publisher: AON (2002-2009), ISBN: 83-88062-23-9, [online]

<http://web.archive.org/web/20181211124349/https://mkuliczkowski.pl/static/pdf/slownik.pdf> [accessed on 10.10.2020].

STAWARZ, N. 2020. Beasts in human skin. Japanese crimes during World War II, [online] https://histmag.org/Bestie-w-ludzkiej-skorze-Japonskie-zbrodnie-w-czasie-II-wojny-swiatowej-21009 (access: 10.10.2020).

SZPAK, A. 2008. "Civilian population" in the context of crimes against humanity in the ruling of the International Criminal Tribunal for Crimes in the former Yugoslavia in the case of Milan Martić (2008), " Review of Public Law " 2009, No. 6, pp. 62-68. [online] https://sip.lex.pl/komarzenia-i-publikacje/artykuly/-ludnosc-cywilna-w-kontekscie-zbrodni-praszko-ludzkosci-w-151095461(access: 10.10.2020).

The Cartagena Declaration of November 22, 1984, [online] https://www.unhcr.org/about-us/background/45dc19084/cartagena-declaration-refugees-adopted-colloquium-international-protection.html (accessed: 24/09. 2022).

UN Information Center in Warsaw, International Criminal Tribunal for the former Yugoslavia - origins and goals, [online] https://www.unic.un.org.pl/prawa-czlowieka/miedzynarodowy-trybunal-karny-dla-bylej-jugoslawii/3158, (access: 20/09/2022).

Wars in cities: protection of civilians in urban settings, 2022, [online] https://www.icrc.org/en/document/wars-cities-protection-civilians-urban-settings (access: 20/09/2022).

WIATR, K. 2020. African humanitarian organizations criticize the peace mission in Darfur, [online] https://www.unic.un.org.pl/misje_pokojowe/unamid.php (accessed: 10/10/2020).

Mgr. Bożena KONECKA-SZYDEŁKO,
UMB v Banska Bistrica: Department of International Relations.
Národná 12, 974 01 Banská Bystrica, Slovakia,
ORCID number: 0000-0001-8018-6973
e-mail: Bozena.Konecka-Szydelko@sanepid.gov.pl

Mgr. Dorota WŁODYKA-TYCZYŃSKA
Economy Office As Property of the City of Rzeszów,
Plac Victims of the Ghetto 3, 35-002 Rzeszów, Poland,
e-mail: dorota.wlodyka@wp.pl

DEVELOPMENT OF AIR DEFENCE MISSILE PLANNING CAPABILITIES IN UNIVERSITY OF PUBLIC SERVICE (HUNGARY)

Zoltan KRAJNC, Janos CSENGERI, Erika VALLUS

ABSTRACT

The article and presentation of the 13th International scientific conference 'National and International Security 2022' summarized a project aimed development of air defence missile capabilities in the University of Public Service (Budapest, Hungary). The development team consisting of anti-aircraft missile and flying tactical specialists and IT-experts develop an operational planner support infrastructure. This future infrastructure (Air Defence Missile Planning Laboratory equipped with special application for studying and analysing of tactical situations) will be able to support the air force and anti-aircraft tactical analysis and planning competencies of air defense missile cadets. The laboratory will be based on a special software developed on the basis of ArcGIS, which is a family of client and server software, and online geographic information system (GIS) services developed and maintained by ESRI Company.

Keywords: air defence planning, core air defence missile capabilities, software development, laboratory building, military cadet training

INTRODUCTION AND PURPOSE OF RESEARCHES[1]

Under the 2021 Thematic Excellence Programme, the National Research, Development and Innovation Fund (Hungary) will support the research of 39 knowledge dissemination organisations in 80 thematic areas, worth around HUF 75 billion.

The aim of the TKP 2021 is for knowledge dissemination organisations to build on their professional excellence and carry out thematic research and development programmes (including basic research, applied research and experimental development) in order to lots of general aims including:

- develop a product, prototype, technology or service with significant scientific and/or technical novelty;
- make the product, technology or service resulting from the thematic research commercially viable;
- improve the research conditions;
- increase scientific productivity.

The number of project proposals supported per sub-programme is 29 in the Health sub-programme, 27 in the National Research sub-programme, and 24 in the National Defence, National Security sub-programme.

Our research and development task is carried out within the framework of National Defence, National Security sub-programme awarded by the Faculty of Military Science and Officer Training of the National University of Public Service, Budapest (Hungary).

[1] Project no.TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

Project no.TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

Title of the project: “Applied military technical, military and social science research in the field of national defense and national security at the Faculty of Military Science and Officer Training.”

Focus and cooperation, the research tasks of military science in the study, the current topics of Hungarian military science were identified by some eminent representatives of the Hungarian military and security science. (Boda, Boldizsár, Kovács, Orosz, Padányi, Resperger, Szenes, 2016)

According to the analysis, six common, future research directions can be identified:

- strategic leadership,
- the armed forces of the future,
- the challenges of hybrid warfare,
- the humanities of the forces,
- the use of modern technology in the military,
- and regional geopolitical crises.

Our research task is closely related to the use of modern technology in the military and the armed forces of the future subtopics. It can be concluded that knowledge of international trends in the field of military science is essential, because otherwise it is not possible to ensure modern force development and the fulfilment of interoperability requirements in multinational operations.

Firstly I would like to summarize of the general objective and structure of the major project. The concept of broader security has previously overshadowed the issue of military security, but the processes of recent years (arms race, mass migration, challenges arising from environmental change) have brought the military segment back to the fore. The topic is highlighted by the importance of the military's national defence tasks, the new national military strategy and compliance with the requirements of the National Defence and Force Development Programme. The subject of the research is also related to the development of the defense administration system, which is considered one of the priority government intentions today. The main objective of our program is to strengthen Hungary processes aimed at developing its security and defense capabilities especially in the field of military research and education.

The expected results of our research will be realized in products (prototype, software) and procedures, strategic evaluations and government decision-making proposals as planned.

The university project works in 4 so-called Highlighted Research Areas (hereinafter: HRA) and 4 Research Groups (RGs) to implement tools, procedures and responses to defence challenges that are directly useful for the defence sector and, in the long term, fit into the goals of our military strategy and the Zrínyi Defence and Force Development Programme. Research on the "Integrated Sample Airport" HRA1 focuses on the development of integrated, safe and environmentally sound airport operating conditions for conventional and unmanned aircraft.

"Capabilities and knowledge-based systems supporting tactical decision-making" HRA2 is developing a knowledge-based system for planning and decision support missions.

"Application of 3D metal printing in military logistics and the military industry" HRA3 is looking for cost-effective solutions by printing weapons and automotive parts locally.

The HRA4 named the "Application of Artificial Intelligence, Alternative Realities and Radio Frequency Techniques for Defence Purposes" aims to develop systems for defence purposes based on AI, xR and RF.

The “International Defence Framework of Europe and Hungary – Opportunities of Strategic Autonomy” research group (RG1) aims at the complex analysis of threats against international peace and security in a constantly changing and multilateral international environment, and the responses given to them.

"Applied Science" RG2 aims to analyze data from military and civilian satellites and mega constellations, including ionizing radiations and their theoretical and logical aspects of relativity.

The aim of the RG3 "Defence and Security Regulations Reform 2023" is to analyze the defense-security system in force from 2023, to develop development proposals.

"Regional synergies of national defence and force development efforts and opportunities for joint action in Central and Eastern Europe" RG4 aims to interpret the current processes of the CEE region, including Hungary its immediate environment, through the small-state debate and using the relevant literature.

The all research work and this article will be realized within the framework of the project TKP2021-NVA-16, with the support of the National Research Development and Innovation Fund (Hungary), funded by the Thematic Excellence Program 2021.

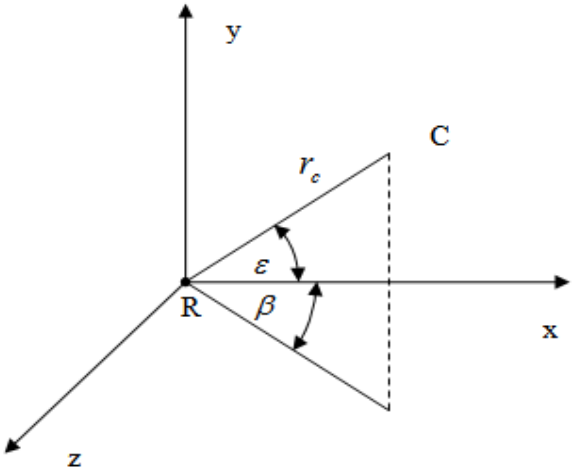
1 METHODS

The second Highlighted Research Area named "the Research for the development of simulation capabilities and expert systems supporting tactical decision-making" carries out developments in order to create a knowledge-based system for air defense missile deployments and decision support. The specific planned result of the research and development will be a special software (application), which will provide an opportunity for specialists dealing with the issues of air defense missile and air force operational tactical application, as well as for persons involved in training and preparation, to analyze and model the tactical possibilities of an anti-aircraft missile grouping in a tactical situation.

Our research is based on the kinematic model of anti-aircraft missile systems, where the determination of the trajectory is the basic task.

To determine the trajectory (with an accuracy of at least 10%), more than 100 non-linear differential equations would have to be written down, so we introduce simplifying conditions for our tests:

- kinematic study of the missile launch (this means dispensing with the dimensions of the rocket and considering the missile as a mass point);
- the missile guidance system is considered ideal (inertia-free);
- all sorts of embarrassment characteristics are dispensed with;
- in the three-dimensional coordinate system, it is best to determine the parameters of the target and rocket based on 2 angles and 1 oblique distance.
- it is enough to conduct the study of kinematic equations only in one plane, since the two planes are analogous to each other;
- based on them, the kinematic equations of the rocket are studied only in the vertical plane;
- the results obtained can be transposed to the other plane.

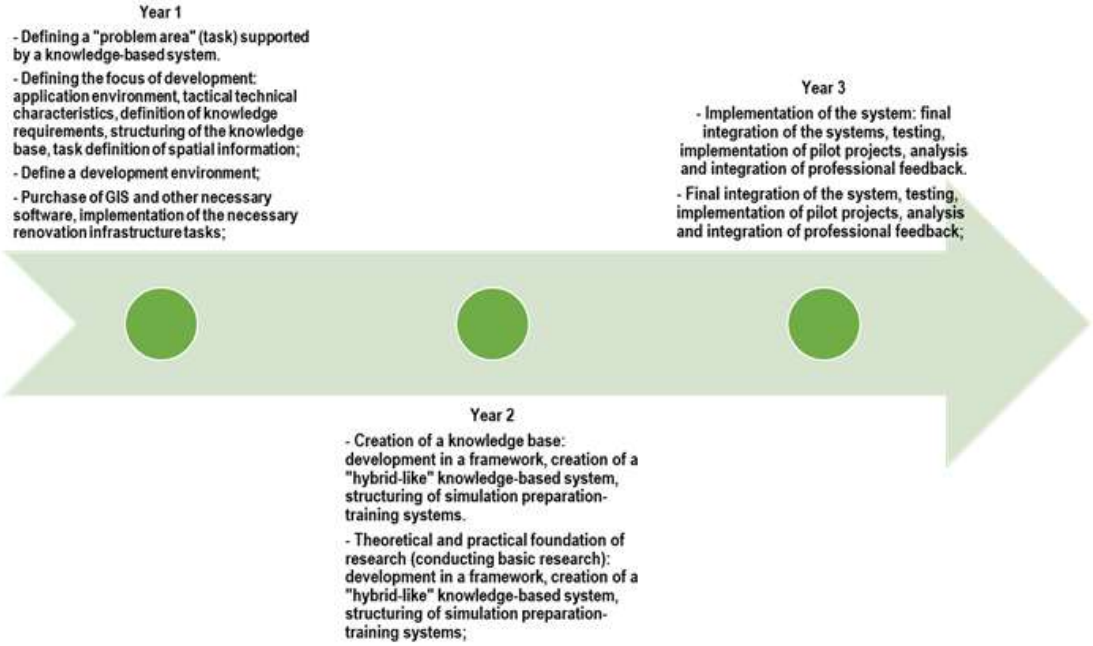


Beta - side angle
Epszilon -location angle
R_c - inclined distance
h_c - altitude

Picture 1 Kinematics of anti-aircraft missiles
Source: Stachó 1992, p. 108.

It is necessary to determine the forces and moments acting on the rocket, and then, based on them, we can study the equations of rocket motion.

For the theoretical foundations, we used the basic works of the topic in Hungary. (Stachó 1992, p. 108, and Fodor 2006, p. 28).



Picture 2 Timetable of Project
Source: Edited by Authors

We have adapted a Scrum framework for our relationships for our development works.

Scrum is an agile product development framework that helps teams solve complex, difficult-to-plan problems and deliver innovative solutions with the highest quality possible. Scrum is a system based on a relatively simple model, which is easy to understand, but extremely difficult to apply well. The Scrum framework consists of the Scrum team and the

roles, events, and tools and rules within it. Because Scrum is a framework, it leaves open the practical ways teams can work for successful product development.

The participants of the Scrum team are the product owner, the scrum master and the development team. Scrum are self-organized, that is, they themselves determine how to achieve their goals, rather than working under external management. Another peculiarity of Scrum teams is cross functionality. This means that the team has all the expertise necessary to deliver a product that works at regular intervals. So, the team's ability to deliver does not depend on any external experts or expertise. For example, a scrum team that develops software can consist of people with the following competencies:

- Software developers who are knowledgeable about the given platform, including front-end, back-end areas.
- Business analysts they are experts who carry out a detailed understanding, specification of user needs. In smaller projects, they often assume the role of product owner. Testers: specialists conducting systematic testing of the software. Manual, automated tests are planned and carried out. Sometimes it is they who also carry out the assembly of the product for release.
- Technical writer is a specialist in the professional preparation of documentation related to the product.
- UX/UI designer is a professional who designs and implements user interfaces and user experiences. (CSUTORÁS, ÁRVAI, NOVÁK 2010, p. 29)

2 STRUCTURE OF AIMED APPLICATION

The planned GIS-based knowledge-based system consists of the 2 main segments:

- Composite Air Operations (COMAO) segment; and
- Anti-aircraft missile fire and reconnaissance system design-analysis segment.

The COMAO segment is made up of following modules:

- Air warfare doctrinal element module:
  - air force concept, air force theories: facilitating understanding of air force application principles, shedding light on the origins of the principles;
  - types of air operations with fitted case studies: to promote an understanding of the state-of-the-art application of the Air Force, enable an overview of the main areas of application and type of tasks of the Air Force;
  - typical air warfare assets by country, alliance, region by task type: specify the design base (database) for complex air operations;
- COMAO-planning module : be able to compile the selected COMAO type and the impact to be achieved, assign targets, route planning, strike plotting, aggregating the damage caused and determining own losses;

Detailed information about COMAO can be obtained from Frederiksen's study. (Frederiksen 2018)

The Anti-air.craft missile fire and reconnaissance system design-analysis segment comprises in:

- Weapons systems:
  - by country, region, alliance level;
  - by purpose (by typical task);
  - modes of control of anti-aircraft missile weapons;
  - basics of kinematics of anti-aircraft missiles;
- Air defense missile evaluation of defended objects:

    - type objects;
    - case studies;
- Summary of the doctrinal principles of anti-aircraft missile application (tactics)
    - tactical employment guidelines;
    - combat order design;
    - fire and reconnaissance system design;
- "Static" combat opportunity evaluation;
- "Quasi-dynamic" combat opportunity evaluation;

In the preparation of combat activity, determining an organization's capabilities to carry out tasks and the resources to ensure their realization is one of the most complex, complex in context, most significant problems of command work. The fundamental reason for this is that the category of indicators of capabilities for task execution includes not only those objectified, tangible elements whose values and possibilities can be easily determined on the basis of tactical technical data of the regular technical means, but also the capabilities characteristic of the given organization, sometimes without any numerical indicators, and their characteristics, which predestine the combat application of the organization under consideration effectiveness.

The literature on the tactics of anti-aircraft missile units characterizes the capabilities for task execution with the so-called combat capabilities of the relevant organizations. The combat options can be quantified quantitatively, and they characterize as a qualitative indicator the ability of the anti-aircraft missile unit – under different conditions – to perform the combat task. This ability is basically determined by the replenishment of the personnel of a given organization, their preparedness, as well as the technical parameters of the available technical means.

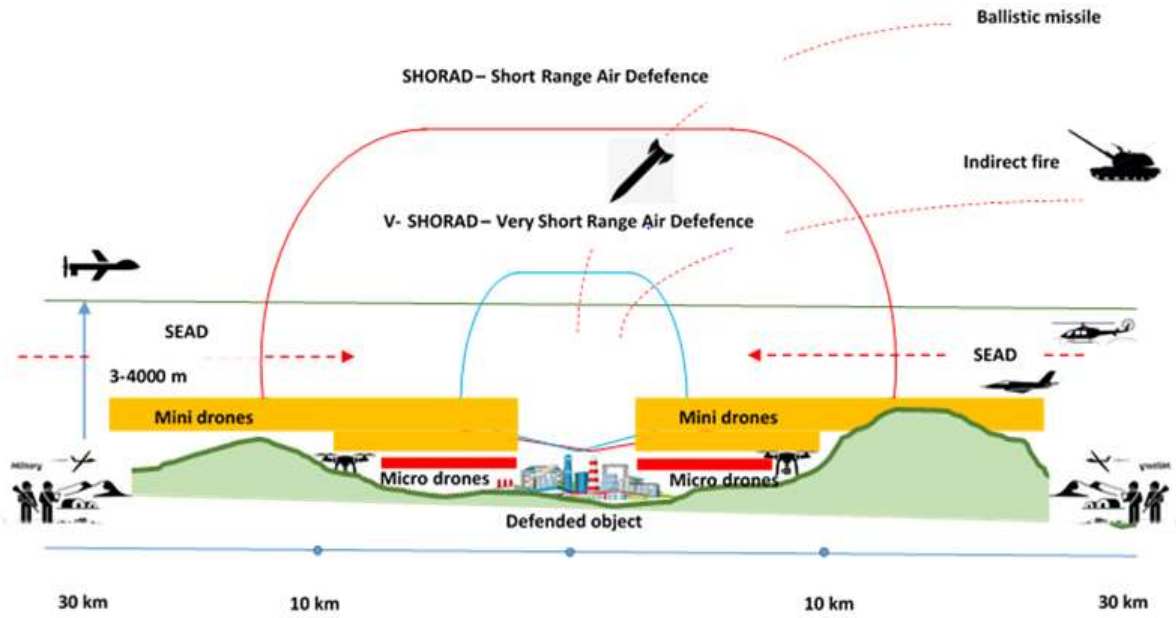
3 DISCUSSION AND CONCLUSIONS

Combat options can be considered basically in two approaches. According to one of them, the tasks to be solved by the anti-aircraft missile unit are determined as an expectation, a requirement, the combat options necessary for the execution of a given task. In the other case, based on the actual combat capabilities of the anti-aircraft missile unit, the requirements that can be imposed on the unit under consideration are the result data of the analysis. Since the primary issue of any command decision is knowledge of the combat capabilities of subordinate organizations, the accurate definition and analysis of their indicators is also a key issue for leadership.

There are a lot of components of combat options that could be listed that can more or less characterize the ability of a particular anti-aircraft missile unit to perform a combat task and, consequently, to meet the requirements imposed on it. However, starting from the fact that the air defense missile unit is able to have the desired effect on the air enemy only if it has the information and energy necessary to perform the task in the right place at the right time, it is also advisable to group the combat options accordingly, as follows:

- the possibility of obtaining information necessary for the execution of the task:
    - the possibility of reconnaissance;
    - the possibility of transition to rocket launch readiness;
    - the possibility of performing maneuvers with forces and devices;
- the possibility of destroying airborne means of attack:
    - the number of firings that can be fired;
    - firing efficiency;
- possibility of protection:

- the size of the protection sector or the width of the protection band;
- the average coverage and structure of the fire zone.



Picture 3 Complex environment of employment of anti-aircraft weapons
Source: Edited by Authors

Publications on the combat capabilities of anti-aircraft missile units do not take a unified position on the issue of combat capabilities or their indicators. Some list more ingredients than before, and others list fewer ingredients. The complexity of the problem is characterized by the fact that even on the issue of the possibility of detection, the position of specialists is not uniform. Despite the fact that some question even the idea of including the possibility of reconnaissance among combat options, it clearly falls into this category as an indicator characterizing the possibility of obtaining information necessary for the execution of the task. Of course, we must treat as a sub-indicator of this area of combat possibilities all opportunities characterized by time factors, such as the possibility of switching to missile launch readiness, as well as the possibility of performing manoeuvres with forces and means.

Determining combat options is a task that requires great care. If, during the period of their preparation, during the development of the command decision and the assignment of tasks to subordinates, we miscalculate or determine the combat capabilities of the anti-aircraft missile unit, then this may have unpredictable consequences during the implementation of combat activities. However, the first step in this process must always be a concrete definition of needs, precisely because of the realistic requirement.

Options for use of indicators of combat opportunity: looking at the issue in more detail, we can see that in the literature we can find basically two approaches to determining the combat options and their indicators. According to one of them, indicators of combat possibilities are obtained in the case of approaching the considered missile unit from the capabilities. These are the so-called potential combat options.

Potential combat options can be quantified quantitatively, and as a qualitative indicator characterize the maximum capability of an air defense missile unit during the implementation of combat activities.

In this case, combat options, respectively, their indicators can qualify the anti-aircraft missile unit only in terms of potential capabilities to perform tasks. However, the prognosis of the extent to which an organisation is capable of carrying out the tasks assigned in the event

of an armed struggle, with its available forces and means, can only be made with the help of test methods and indicators obtained as a result thereof, in which, in addition to the resources available to the opposing parties, their expected activities are taken into account in some way. This idea is reflected in the approach according to the other logic, where the combat possibilities and their indicators are determined taking into account the influencing, limiting effects of the environment. These are the so-called realizable combat options.

Realizable combat options characterize as a numerically expressable quantitative and qualitative indicator the expected value of the capabilities of the air defense missile unit for task execution during the execution of combat activity.

Of course, it is not possible to dispute the correctness of any test method, however, the possibilities of using their result data and the objective content of their meaning are different. While the potential combat capabilities of anti-aircraft missile units primarily provide easy and quickly definable data for the large-scale, relatively realistic tasking of the command level, which also assesses the needs, the realizable combat possibilities, assuming a specific environment, taking into account its limiting effects, approximately predict the results of the task execution of the air defense missile unit. The combat possibilities that can be realized can also serve as feedback on the task-setting of the leader, thus creating a harmony of requirements and possibilities.

Before examining the definition of realizable combat options, it is absolutely necessary, for the sake of some thoughts, to clarify the problem that arises around the definition of combat possibilities and the application of the theory of evaluating the established fire system.

The problem is basically the mixing of combat options and indicators of the created fire system. Despite the fact that they are two studies with completely different philosophies, occasionally already when analyzing the combat capabilities of anti-aircraft missile units, they try to determine the characteristics of the created fire system, that is, they interpret the fire system indicators as indicators of combat possibility. Perhaps the best way to clarify the issue is to interpret the study of combat capabilities as a static analysis of anti-aircraft missile units and to treat the results obtained as the maximum or expected value of the anti-aircraft missile unit's ability to perform a combat task. In contrast, when evaluating the created fire system, the missile unit is examined in the dynamics of the implementation of the combat task, and the result data obtained will be characteristics of the effectiveness of a set specific situation.

Although during the dynamic evaluation of anti-aircraft missile units – assuming a specific situation, but only for that one situation – we can obtain significantly more realistic data, of course we cannot dispense with static testing either, since its results – using fewer but fundamental probability variables – factually characterize the ability of the missile unit to perform the combat task assigned to it.

There is a realistic need to develop a test method that would combine the advantageous properties of the static and dynamic test method as optimally as possible, i.e. the values obtained as a result of its application would reflect the combat capabilities of the anti-aircraft missile units more realistically than the indicators of potential combat capability , projecting the activity of the air enemy to some extent, but at the same time, contrary to the assessment of the fire system created, they wouldn't just apply to a specific situation that's likely.

Since the realizable combat capabilities of anti-aircraft missile units presuppose the effects of environmental elements that reduce potential combat possibilities, the data obtained as a result of their determination necessarily meet the above requirements, thereby allowing the development of a more realistic command decision. However, it should be stressed that since probabilistic variables are used in the calculations as regards environmental compartments, the result data obtained are only expected values.

As a result of the planned development project, we will receive a specialized laboratory in which the tactics competencies of our cadets will be well developed. They will be able to plan the combat employment of anti-aircraft missile fire subunits, optimize decision-making combat options, as well as model air enemies. In addition to competence development, the laboratory and specialized software will also allow the analysis of tactical situations, such as:

- projected airborne threat modelling;
- possible COMAOs determination;
- to support the air defense assessment of the object to be protected;
- to optimize the operating model of anti-aircraft missile fire subunits;
- data-based evaluation of tactical decisions.

BIBLIOGRAPHY

BODA, J. - BOLDIZSÁR, G. - KOVÁCS, L. – OROSZ, Z. – PADÁNYI, J. – RESPERGER, I. – SZENES, Z. Focus and cooperation, the research tasks of military science, Hadtudományi Szemle, 2016/3. (chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://real.mtak.hu/124069/1/HSZ_2016_144_3_Boda_Jozsef.pdf, downloaded 30 Sep 2022)

STACHÓ, T. Légvédelmi Rakéták Rendszertana I. Bolyai János Katonai Műszaki Főiskola, Budapest, 1992.

STACHÓ, T. Légvédelmi Rakéták Rendszertana II. Bolyai János Katonai Műszaki Főiskola, Budapest, 1992.

FODOR, G. Jelek és rendszerek, Műegyetemi Kiadó, Budapest 2006.

CSUTORÁS, Z. - ÁRVAI, Z. - NOVÁK, I. A Scrum keretrendszer és agilis módszerek használata a Visual Studióval, Devportal Kiadó, 2010.

KRAJNC, Z. – CSENGERI, J. Hybrid warfare from military air perspective, MORONG (ed.) 8. Medzinárodná Vedecká Konferencia: "National And International Security 2017", Liptovsky Mikulas, Szlovákia : Akadémia ozbrojených síl generála Milana Rastislava Štefánika (2017) 614 p. pp. 254-262. , 9 p.

FREDRIKSEN, P. K. Interaction in Aerial Warfare: The Role of the Mission Commander in Composite Air Operations (COMAO), Royal Norwegian Air Force Academy, 2018.

KRAJNC, Z. - CSENGERI, J. Early concepts and theories of employment of air power, MORONG (ed.) 12. Medzinárodná Vedecko-Odborná Konferencia: Management - Theory, Education and Practise 2016, Liptovsky Mikulas, Szlovákia : Akadémia ozbrojených síl generála Milana Rastislava Štefánika (2016) 346 p. pp. 164-171. , 8 p.;

KRAJNC, Z. – RUTTAI, L A légtér feletti ellenőrzés képességének szintjei, Repüléstudományi Közlemények (2002)2 pp. 125-131. , 7 p.;

KRAJNC, Z. –RUTTAI, L. A magyar légierő doktrinális alapjai, Budapest, Magyarország : Zrínyi Miklós Nemzetvédelmi Egyetem (2001) , 63 p.;

KRAJNC, Z. – BERKOVICS, G. –KOCZKA, J. A magyar légvédelem „szeme és füle”: 1917 – 1945, Haditechnika (2006) 2 pp. 1-8. , 8 p.

Colonel Zoltan KRAJNC (PhD) University Professor, Vice Dean of Academic Affairs of University of Public Service, Military Science and Officer Training Faculty
Hungary - 1083 Budapest, 2 Ludovika tér
E-mail krajnc.zoltan@uni-nke.hu

Lieutenant Colonel Erika VALLUS PhD-student, University of Public Service, Military Science and Officer Training Faculty
Hungary - 1083 Budapest, 2 Ludovika tér
E-mail vallus.erika@mil.hu

Captain János CSENGERI (PhD) Assistant Professor, University of Public Service, Military Science and Officer Training Faculty
Hungary - 1083 Budapest, 2 Ludovika tér
E-mail csengeri.janos@uni-nke.hu

POKROČILÉ MOBILIZAČNÍ PLÁNOVÁNÍ: POŽADAVEK NA URYCHLENÍ ROZVOJE SCHOPNOSTÍ OZBROJENÝCH SIL?

ADVANCING MOBILIZATION PLANNING: THE REQUIREMENT TO ACCELERATE THE DEVELOPMENT OF THE CAPABILITIES OF THE ARMED FORCES?

Petr KŘÍŽEK, Fabian BAXA, Vladimír VYKLICKÝ, Aleš TESAŘ

ABSTRACT

Based on the experience of securing the operation of the country during the COVID-19 pandemic and the current events in Ukraine, it is necessary to urgently resolve issues related to mobilization planning from the point of view of the development and maintenance of the capabilities of the armed forces, the economy of state defence and the protection of the population in the event of a crisis. These events changed the view of political representation on the need for ready plans and human and material resources in case of the need to accelerate the development of the capabilities of the armed forces. Therefore, today it is necessary to look at securing the mobilization and development of the armed forces capabilities to solve sudden security problems. This article has the ambition to open an expert discussion on these questions.

Keywords: capability, mobilization, planning, resources, security

ÚVOD

Česká republika, podobně jako ostatní státy Evropské unie, v posledním období čelila nepokojům obyvatel vyvolávaným z důvodu přijímání protiepidemických opatření při ochraně obyvatelstva proti COVID-19. Po mírném uklidnění pandemické situace vznikl na východní hranici EU válečný konflikt, který je doprovázený energetickou krizí. Válečný konflikt, který je sám osobě bezprecedentním ohrožením bezpečnosti v Evropě, a s ním spojená energetická krize jsou také živnou půdou pro růst hrozeb pro evropskou bezpečnost, a to počínaje terorismem, násilným extremismem, organizovaným zločinem a konče hybridními konflikty, kybernetickými útoky, migrací, šířením zbraní a nekontrolovatelným pohybem migrantů a zbraní po evropském kontinentu. Od skončení studené války, se tak státy EU ocitly v situaci, kdy jsou výrazným způsobem ohroženy bezpečnostní zájmy EU a jejich jednotlivých členských zemí, a to především ochrana demokracie a právního státu a zajištění bezpečnosti obyvatel.

I přesto, že ČR je členem NATO, čímž má zajištěnu obranu země v rámci kolektivního závazku, je zapotřebí mít stále na zřeteli otázku mobilizace a mobilizačního plánování jako nedílné součásti zabezpečení potřebných zdrojů ve prospěch obrany státu, a to především lidských a materiálních. Současné dění v jižní části Evropy, kde dochází ke zvyšování napětí mezi dvěma členskými státy Aliance, ukazuje, že se nelze v dnešní době zcela spoléhat pouze na princip kolektivní obrany. Je skutečností, že válečný konflikt velmi výrazně napomohl k semknutí evropských států proti agresorovi, ale nelze zapomínat na úskalí doprovázející dopady pandemie COVID-19 na chod jednotlivých států. Zahájená politická diskuze k tématům, která souvisí s přípravou státu na svoji obranu, je tak na místě. (NATO, 2022)

Česká legislativa se o obraně státu a mobilizaci vyjadřuje následovně: Obrana státu představuje souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie

a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil státu a prostředků a účast v kolektivním obranném systému. (Zákon č. 222/1999 Sb.) Dle zákona č. 222/1999 Sb., o zajišťování obrany České republiky, naplnění obrany státu zahrnuje výstavbu, přípravu a řízení ozbrojených sil, operační přípravu státního území, plánování obrany státu a opatření v národním hospodářství a na všech úsecích veřejného života v zájmu zajišťování obrany státu. (Zákon č. 222/1999 Sb.)

Ve znění výše uvedeného zákona se plánováním obrany státu rozumí *„soubor plánovaných opatření, vzájemně se ovlivňujících, k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením a ke splnění všech požadavků na zajišťování obrany státu, zabezpečení mezinárodních smluvních závazků o společné obraně, včetně podílu ozbrojených sil na činnostech mezinárodních organizací ve prospěch míru a účasti na mírových operacích“*. Plány obrany jsou dle zákona o zajišťování obrany České republiky., tvořeny obranným plánováním, plánováním operací, mobilizačním plánováním a plánováním připravenosti obranného systému státu. (Zákon č. 222/1999 Sb.)

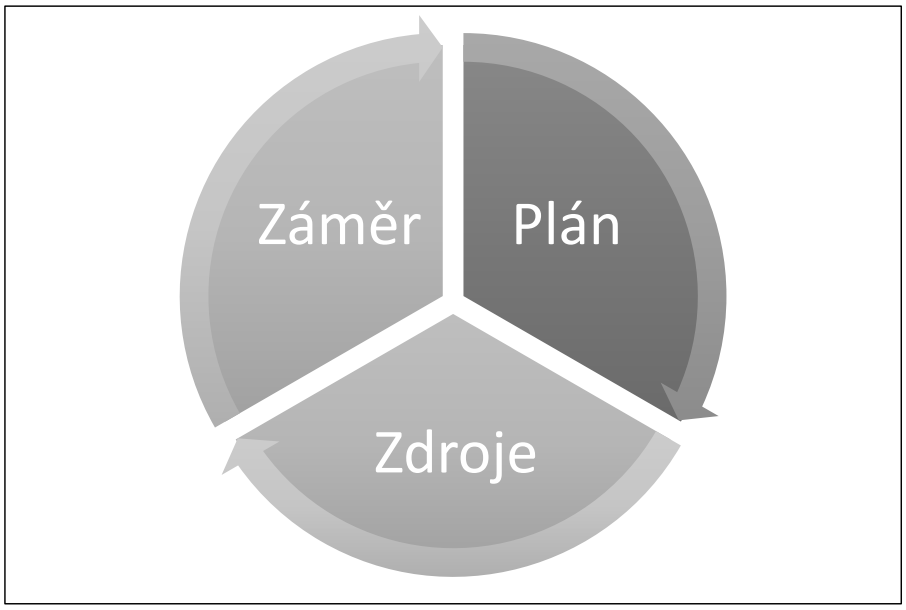
Před řešením pandemie COVID-19 se mobilizační plánování a vlastní mobilizace jevily jako nepotřebné a díky členství ČR v EU a NATO se dokonce hovořilo o mobilizaci jako o přežitku minulé doby. Cílem tohoto článku je podívat se na mobilizaci, hospodářskou mobilizaci a mobilizační plánování v kontextu aktuálního dění.

1 MOBILIZACE A MOBILIZAČNÍ PLÁNOVÁNÍ V SOUČASNOSTI

Samotný pojem mobilizace je velmi starý pojem pocházející z latiny a znamenající uvedení někoho nebo něčeho v pohyb. Mobilizace je tak procesem v přípravě sil a prostředků na řešení bezpečnostních hrozeb. Za procesní přístup je považováno aplikování procesů v organizaci, v tomto případě ve státě a následně v resortu MO, s jejich identifikací a vzájemným propojením. Mobilizace tak označuje proces přípravy na vedení ozbrojeného konfliktu, přičemž obecně může označovat přípravu na činnost, pro kterou nejsou z běžného stavu dostupné dostatečné síly a schopnosti.

V prostředí obrany ČR se jedná o zajištění přechodu státu z mírového stavu do stavu ohrožení státu nebo válečného stavu uvedením ozbrojených sil ČR do vyšších stupňů pohotovosti a jejich převedení z mírové do válečné organizační struktury. V civilním prostředí se jedná o systém hospodářských opatření pro krizové stavy v bezpečnostním systému ČR, takzvaná hospodářská mobilizace.

Dle zákona č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon) se hovoří o mobilizaci ozbrojených sil jako o hromadném povolávání vojáků v záloze do mimořádné služby. Mobilizace ozbrojených sil může být částečná nebo všeobecná. Částečná mobilizace ozbrojených sil ČR se za stavu ohrožení státu vztahuje na část vojáků v záloze nebo na část státního území České republiky. Všeobecná mobilizace ozbrojených sil ČR se za válečného stavu vztahuje na všechny vojáky v záloze. Vojákem v záloze se stane muž či žena ve věku od 18 do 60 let, který dobrovolně převezme výkon branné povinnosti. Branný zákon definuje brannou povinnost jako povinnost státního občana ČR, který za stavu ohrožení státu nebo válečného stavu vykonává mimořádnou službu. (Zákon č. 585/20004 Sb.)



Obrázek 1 Zajištění mobilizačních zdrojů

2 HISTORIE MOBILIZACE NA ÚZEMÍ ČR

V období balkánských válek (1911-1913) mobilizoval každý stát účastnící se přípravy na válku s Osmanskou říší. (Štěpánek, 2022) Na bouřlivý vývoj balkánských válek a probíhajících mobilizací v Rusku, Turecku, Řecku a Černé Hoře reagovalo Rakousko-Uhersko vyhlášením částečné mobilizace v prosinci 1912. Následně v červenci 1914 poté, co rakousko-uherská monarchie neuznala srbskou odpověď na ultimátum, podepsal císař František Josef I. rozkaz o částečné mobilizaci. Mobilizace ale zdaleka neproběhla tak hladce, jak si rakouské velení představovalo a nadšení mladých branců rozhodně nebylo všeobecné. Aby byl zajištěn klidný průběh mobilizace, vyhlásil císař výjimečný stav. V důsledku něho byla výrazně omezena osobní svoboda každého obyvatele rakousko-uherského mocnářství. Vzhledem k tomu, že Čechy a Morava byly součástí Rakousko-Uherské monarchie, týkalo se vyhlášení mobilizace i zemí Koruny české. (Štěpánek, 2022)

Po ukončení první světové války se v Československu situace uklidnila. Tento relativní klid trval až do roku 1936, kdy dění v Německu zásadně ovlivňovalo českou politiku a vývoj rozpočtu na budování obrany a rozvoj ozbrojených sil. V důsledku Květnové krize roku 1938, která byla způsobená zprávami o pohybech německých vojsk proti Československu a zprávami o bezprostřední hrozbě vypuknutí války v Evropě, byla dne 20. května 1938 vyhlášena jak částečná mobilizace v Československé republice, tak zvýšená ostraha státní hranice. Povoláno bylo na 180 000 vojáků v záloze na zajištění nedostatečně obsazených postů na státní hranici. Armáda tak ve velmi krátké době byla schopna navýšit své počty na 380 000 osob. Po uklidnění situace, v červnu 1938, byli vojáci ze státní hranice staženi a vojáci v záloze propuštěni domů.

Další vývoj událostí v Německu vedl k tomu, že prezident Československé republiky vyhlásil 23. září 1938 v nočních hodinách mobilizaci. (Straka, 2020) Tato mobilizace povolala 18 ročníků I. zálohy a náhradní zálohy všech zbraní a služeb a dále také část příslušníků II. zálohy, která se týkala potřebných specialistů. Celkem bylo povoláno 1 250 000 mužů do zbraně

včetně těch, kteří byli povoláni již před začátkem mobilizace. Mobilizačně rozvinuté síly měly k dispozici 350 tanků, 5000 dělostřeleckých hlavní a 950 bojových letounů.[1]

Před vlastní mobilizací byli vojáci v záloze povoláváni na mimořádná cvičení ve čtyřech vlnách. 20. května 1938 bylo na mimořádné cvičení ostrahy státní hranice povoláno na 28 tisíc mužů, kteří se dostavili na své pozice nejpozději druhý den ráno. Dne 12. září 1938 byla vyhlášena zvýšená pohotovost a na mimořádné cvičení bylo povoláno dalších 240 tisíc mužů, následující den vyhlášení bylo povoláno dalších 120 tisíc mužů. Dne 17. září 1938 se dostavilo dalších 80 tisíc mužů na mimořádné cvičení. Celkem tak bylo od května do září roku 1938 povoláno do zbraně na 1,7 milionu mužů. (Stejskal, 2014)

3 ANALÝZA AKTUÁLNÍHO STAVU MOBILIZACE V ČR

V posledních letech se v politických i vojenských kruzích hodně diskutovala otázka, zdali se zabývat problematikou mobilizace. Většina politiků, ve vojenských kruzích již méně, se díky našemu členství v kolektivní obraně přikláněla k názoru, že se jedná o přežitek. (Stejskal, 2014) Bohužel skutečnost je taková, že pro zajištění přechodu ozbrojených sil ČR z mírové organizace na válečnou strukturu je nezbytné provést celou řadu činností, jež jsou zahrnovány do pojmu proces mobilizace. V souladu s branným zákonem se mobilizace týká pouze doplňování ozbrojených sil ČR lidskými zdroji. (Zákon č. 585/2004 Sb.) Zde je potřeba si uvědomit, že pro doplnění lidskými zdroji je nezbytné také zajistit materiálové a peněžní zdroje.

Po vzniku válečného konfliktu na Ukrajině se ukazuje, že v celé Evropě vyvstala vysoká poptávka po materiálních zdrojích na zajištění systému bezpečnosti států, což má za následek jejich nedostatek. Přestože státy bývalého východního bloku donedávna ještě disponovaly přebytky materiálních zdrojů z doby Varšavské smlouvy, byl jejich technický stav na velmi nízké úrovni. Zabezpečit moderní zbraně a zbraňové systémy v době válečné krize se tak stává velmi finančně a časově náročnou záležitostí. Proto k zajištění některých materiálních zdrojů tak Česká republika využívá statutu hospodářské mobilizace. (Zákon č. 241/2000 Sb.)

Do konce roku 2000 byl v ČR v platnosti systém hospodářské mobilizace, který prošel dvěma vývojovými fázemi. Nejdříve byl do roku 1992 systém založen na direktivním řízení, jehož základním nástrojem byl rozpočtový plán. Následně v tomto roce byla realizována změna na základě Nařízení vlády ČR č. 284/1992 Sb., o opatřeních hospodářské mobilizace, která v podstatě přizpůsobila systém hospodářské mobilizace změněným ekonomickým podmínkám a znamenala přechod od direktivního ke smluvnímu systému. (NV ČSFR č. 284/1992 Sb.) Nově zavedený systém umožnil využití opatření připravovaných pro období branné pohotovosti státu i pro řešení jiných krizových situací a vymezil základní subjekty a nástroje tohoto systému.

Zásadní změnu však přinesla až nová krizová legislativa, která vstoupila v platnost po 1. lednu 2001. Do této krizové legislativy, která je až na dílčí změny vyvolané reformou veřejné správy platná do současnosti, patří rovněž zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů. Současný systém hospodářských opatření pro krizové stavy představuje relativně samostatný a samostatně právně zakotvený systém, který je vzájemně propojen s ostatními prvky bezpečnostního systému ČR a který má přesně vymezené místo a účel v oblasti přípravy a přijetí opatření po vyhlášení krizových stavů.

Koncepce mobilizace ozbrojených sil České republiky mobilizační plánování definuje jako součást plánování obrany státu. Pod daným pojmem si lze představit proces, kterým se stanovuje posloupnost plánovaných opatření a časových lhůt k přípravě a zabezpečení

[1] ČESKÁ TELEVIZE. *Proveďte Zborov-25! Československá armáda dokázala přes noc obsadit celé hranice*. [online] 2018 [cit. 2022-09-04] Dostupné z internetu: https://1url.cz/7rpOT.

doplňování a mobilizace. Zahrnuje plánování všech opatření při respektování požadavků ostatních součástí bezpečnostního systému ČR. Obrana státu je záležitostí všech státních orgánů, orgánů územní samosprávy, právnických osob i občanů. Úkoly a odpovědnost některých subjektů při přípravě k obraně státu před vnějším napadením v míru, za stavu ohrožení státu a za válečného stavu stanovuje také zákon č. 222/1999 Sb., o zajišťování obrany ČR. (MO, 2012)

Systém obrany státu má svá specifika, která se musí odrazit ve struktuře, způsobu a metodách jeho řízení. Je součástí bezpečnostního systému ČR. Systém plánování obrany státu je v rezortu ministerstva obrany chápán jako soubor pěti plánovacích disciplín, které vycházejí z definice zákona o zajišťování obrany. (Zákon č. 222/1999 Sb.)

Dle Koncepce mobilizace ozbrojených sil ČR lze tedy mobilizační plánování chápat jako proces, kterým se stanoví posloupnost plánovaných opatření a časové lhůty k přípravě a zabezpečení doplňování a mobilizace. Zahrnuje plánování všech opatření při respektování požadavků ostatních součástí bezpečnostního systému ČR. (MO, 2012)

V mírovém stavu jsou k doplnění a mobilizaci útvarů válečné organizační struktury zpracovány bilance mírové nenaplněnosti, mobilizační plány rozvinovaných útvarů a mobilizační projekty pro mobilizačně vytvářené útvary. Opatření mobilizačních příprav jsou podrobněji rozpracovány všemi zainteresovanými subjekty.

Před rokem 2004 pro doplnění materiálem rozvinovaných a vytvářených jednotek měl resort obrany materiální zásoby uskladněny. Po roce 2004, z důvodu nedostatku finančních prostředků, a především z důvodu zavádění nové výzbroje, se pro doplnění rozvinovaných jednotek připravovaly mobilizační projekty.

Mobilizační projekt útvaru je soubor podkladových a přehledových dokumentů nezbytných pro zpracování mobilizačního plánu mobilizačně doplňovaného nebo vytvářeného útvaru. Obsahuje základní identifikační údaje, makrostrukturu, záměr doplnění majetku, rozvahu sil a prostředků a další nezbytné údaje. (MO, 2012)

V míru jsou nezbytné finanční prostředky plánovány a vynakládány na definování, vytvoření a aktualizaci mobilizačních projektů, např. příprava vojáků v záloze, provoz informačního systému mobilizačních příprav, skladování nezbytného majetku apod.

V současnosti má resort obrany snahu zahájit plnění mobilizačních projektů ještě dříve, nežli bude vyhlášen stav ohrožení státu nebo válečný stav. Hlavním důvodem je velmi zdlouhavé zabezpečení plnění těchto projektů, které jsou z velké části zajišťovány zahraničními dodavateli.

4 MOBILIZACE A MOBILIZAČNÍ PLÁNOVÁNÍ BUDOUCNOSTI V ČR

Naše společnost se nachází v období tzv. Průmyslu 4,0 a již se začíná hovořit i o Průmyslu 5,0. (Elektroprůmysl, 2022) Tento výrazný technologický pokrok se odráží i v technologickém vývoji zbraní a zbraňových systémů, což se promítá do bezpečnostního napětí nejen mezi velmocemi. Tento technologický rozvoj, společně s dalšími faktory, ovlivňuje myšlení politiků a vojenských představitelů nejen v ČR. Přináší změny v myšlení, které zde bylo po ukončení studené války, kdy došlo k výrazné konverzi zbrojní výroby na jinou strojírenskou výrobu. Z kontextu aktuální situace pak jednou z největších chyb oblasti materiálního zabezpečení zdrojů, bylo zavedení vigilního logistického modelu „just in time“ do vojenské logistiky a zanedbávání většiny válečných zásob. (Dolejší, 2022)

Důsledkem tohoto konání je dnes nedostatek zbraní, zbraňových systémů a munice, nejen pro moderní zbraně, ale i morálně zastaralé zbraně, potřebné pro mobilizaci. Navíc se tento vojenský materiál vyrábí až na objednávku, tudíž až po podpisu smlouvy na danou dodávku. V případě vytváření válečných zásob zbraní a zbraňových systémů v dnešní době stojí jako protipól jejich vytváření velmi rychlý technologický pokrok. Řešením je modernizovat armády postupně a tím zajistit, že v zásobách budou méně zastaralé vojenské systémy.

Cesta, jak toto změnit je v zapojení soukromého zbrojního průmyslu do tvorby a držení nejen válečných zásob, ale i zásob pro jiné krizové stavy státu. Bývalý zástupce velitele ozbrojených sil NATO v Evropě Richard Shirreff upozorňuje na to, že je potřeba *„mobilizovat rezervy*. *Znamená to obnovit schopnosti ztracené v letech, kdy došlo ke snižování výdajů na obranu“*. (Novák, 2022) Je třeba opustit logistický model „just in time“ a začít vytvářet zásoby pro zajištění krizových stavů. Zkušenosti z období pandemie COVID-19 ukázaly, že v případě uzavření hranic jednotlivých států nebylo možné zajistit některý druh potřebného zboží. Navíc události na východě Evropy dále upozorňují na to, jak nebezpečné jsou globalizační výrobní projekty. Většina surovin pro vojenskou výrobu, či většina závodů na jejich zpracování se nacházejí mimo sféru přímého vlivu jak EU, tak NATO.

Základní oblast výzkumu tak bude položena do oblasti analýzy stávajícího právního nastavení zabezpečení mobilizace a nalezení nového právního statusu, především ve vazbě na řešení nalezení legislativního zajištění plnění jednotlivých procesních kroků mobilizace za předem definovaných podmínek. Toto plnění musí být zabezpečeno dříve nežli za stavu ohrožení státu nebo za válečného stavu, z čehož vyplývá potřeba definování nových krizových stavů. Další oblastí zkoumání je najít odpovědi na následující otázky:

- „Kolik nás mobilizace může stát, a to jednak jako celek, ale i jednotlivé etapy jejího životního cyklu?“
- „Máme dostatečné materiální zdroje pro její zabezpečení?“
- „Máme dostatečné lidské zdroje pro její zabezpečení?“

Oblast zkoumání tak bude potřeba řešit nejméně ve dvou rovinách, a to v neutajovaném a v utajovaném režimu. Neutajované výsledky pak bude možné publikovat v odborných časopisech.

Předmětem zkoumání mimo jiné bude i pohled do zahraničí, jak danou problematiku řeší členské země v rámci Aliance nebo EU.

Vzhledem k tomu, že práce by měla být neutajovaného charakteru, dalším předmětem zkoumání bude proces stanovení výpočtu budoucích nákladů na mobilizaci jako druh budování a udržení schopnosti v rámci jejího životního cyklu, tzn. nákladů v době přípravy (v době míru), v době přijímaných opatření (výběrové doplňování) a v době demobilizace. Provést analýzu dostupných zdrojů a na základě jejich výsledků navrhnout model predikce předpokládaných nákladů mobilizace.

ZÁVĚR

Článek splnil svůj cíl, kterým bylo otevřít odbornou diskuzi nad následujícími otázkami: „Jsou stávající plány a plánované zdroje schopny včas reagovat na nenadálé změny, případně jak urychlit mobilizační rozvinování ozbrojených sil?“; „Jaká bude zdrojová náročnost mobilizačního rozvinování?“ a „Má stát k dispozici dostatečné zdroje pro jeho zabezpečení?“.

Z analýzy vyplývá, že otázce mobilizace je potřeba se trvale v budoucnosti věnovat. Zkušenosti s řešením pandemie jednoznačně ukázaly slabá místa státu v řízení právnických subjektů, které jako jedno z opatření hospodářské mobilizace má své opodstatněné místo.

Získané zkušenosti dále ukázaly, že stát v nouzovém stavu nemá žádné nástroje k tomu, jak zabezpečit výrobu potřebného zdravotnického a bezpečnostního materiálu. Nejsou nastavena žádná pravidla pro zkrácený certifikační procedury zdravotnického a bezpečnostního materiálu. Tyto procedury jsou částečně nastaveny v resortu obrany, avšak pouze po vyhlášení stavu ohrožení státu nebo válečného stavu.

Z článku dále vyplývá, že dalšímu zkoumání oblasti mobilizace je nutné v budoucnu věnovat náležitou pozornost a navrhnout potřebná legislativní opatření ke zlepšení řešení velkoplošných krizových situací i za nižších vyhlášených krizových stavů. Za tímto účelem je

potřeba věnovat se i otázkám ekonomického vyčíslení nákladů, které to může zemi stát po dobu celého životního cyklu.

SEZNAM BIBLIOGRAFICKÝCH ODKAZŮ

ČESKÁ REPUBLIKA. *Zákon č. 222/1999 Sb., o zajišťování obrany České republiky*. In: Praha, 1999, 76/1999. [online] [cit. 2022-09-18] Dostupné na internetu: https://www.zakonyprolidi.cz/cs/1999-222.

ČESKÁ REPUBLIKA. *Zákon č. 585/2004 Sb., branný zákon*. In: Praha, 2004, 201/2004. [online] [cit. 2022-09-18] Dostupné z internetu: https://www.zakonyprolidi.cz/cs/2004-585.

ČESKÁ REPUBLIKA. *Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů*. In: Praha, 2000, 73/2000. [online] [cit. 2022-09-18] Dostupné z internetu: https://www.zakonyprolidi.cz/cs/2000-241.

ČESKÁ REPUBLIKA. *Nařízení vlády České a Slovenské Federativní Republiky č. 284/1992 Sb., o opatřeních hospodářské mobilizace*. In: Praha, 1992, 59/1992. [online] [cit. 2022-09-18] Dostupné z internetu: https://www.zakonyprolidi.cz/cs/1992-284.

ČESKÁ TELEVIZE. *Proveďte Zborov-25! Československá armáda dokázala přes noc obsadit celé hranice*. [online] 2018 [cit. 2022-09-04] Dostupné z internetu: https://1url.cz/7rpOT.

DOLEJŠÍ, K. 2022. *Odzbrojený Západ? Bez průmyslové základny jsou vyhlídky konfliktu s Ruskem pochmurné*. [online] 2022. [cit. 2022-09-15] Dostupné z internetu: https://1url.cz/TrpOh.

ELEKTROPRŮMYSL.CZ. *Průmyslová evoluce pokračuje - od Průmyslu 1.0 k Průmyslu 5.0*. [online] 2022 [cit. 2022-09-06] Dostupné z internetu: https://1url.cz/RrpO4. ISSN 2571-0761.

MO. *Koncepce mobilizace OS ČR*. [online] 2012. [cit. 2022-09-18] Dostupné z internetu: https://mocr.army.cz/images/id_40001_50000/46088/koncepce-mobilizace.pdf.

NATO. *NATO 2022: STRATEGIC CONCEPT*. [online] 2022. [cit. 2022-09-18]. Dostupné z internetu: https://www.nato.int/strategic-concept/.

NOVÁK, F. 2022. *NATO není na válku s Ruskem připraveno, varuje bývalý britský generál*. [online] 2022. [cit. 2022-09-20] Dostupné z internetu: https://1url.cz/hrpOR.

STEJSKAL, L. 2014. *Dobrovolná občanská participace při zajišťování obrany: Koncept, zkušenosti a perspektivy*. Obrana a strategie . 2014, roč. 14, č.2, s. 11 9-1 33 . JESN 1802 - 7199. DOI: 10.3849/1802 - 7199.14.2014.02. 11 9-1 33.

STRAKA, K. 2020. *O podstatě a smyslu československé mobilizace z podzimu 1938*. [online] 2020. [cit. 2022-09-05] Dostupné z internetu: http://www.vhu.cz/o-podstate-a-smyslu-ceskoslovenske-mobilizace-z-podzimu-1938/.

ŠTĚPÁNEK, V. 2022. *Albánská otázka a italsko-turecká válka 1911 až 1912*. [online] 2022. [cit. 2022-09-18] Dostupné z internetu: https://1url.cz/SrpOQ.

plk. v.z. Ing. Petr KŘÍŽEK, Ph.D.
Centrum bezpečnostních a vojenskostrategických studií, Univerzita obrany
Kounicova 65
662 10 Brno
petr.krizek@unob.cz

plk. v.v. Ing. Fabian BAXA, Ph.D.
Centrum bezpečnostních a vojenskostrategických studií, Univerzita obrany
Kounicova 65
662 10 Brno
fabian.baxa@unob.cz

plk. Ing. Vladimír VYKLICKÝ
Centrum bezpečnostních a vojenskostrategických studií, Univerzita obrany
Kounicova 65
662 10 Brno
vladimir.vyklicky@unob.cz

Aleš TESAŘ
Centrum bezpečnostních a vojenskostrategických studií, Univerzita obrany
Kounicova 65
662 10 Brno
ales.tesar@unob.cz

DIGITÁLNE STOPY PRI ODHAĽOVANÍ EXTRÉMIZMU SO ZAMERANÍM NA MOBILNÉ ZARIADENIA

DIGITAL FOOTPRINTS IN THE DETECTION OF EXTREMISM FOCUSING ON MOBILE DEVICES

Milan KUSÁK

ABSTRACT

Currently, the vast majority of extremist activity takes place on the Internet. In order for the perpetrators of these crimes to be able to get into the virtual environment and thus spread the hatred associated with extremism among the general population and thus implement communication, extremist groups and individuals, as well as the rest of the population, have to reach for electronic devices for this purpose. For this purpose, they primarily reach for mobile devices, which are the most affordable, storable and it is not a problem to use them from any place in the world where an Internet connection is available or data transmission is possible. This article aims to make the reader aware of the need and increasing trend of examining digital footprints in extremism investigations and related forensic investigations of digital footprints in mobile devices.

Keywords: digital footprints, mobile devices, forensic investigations, extremism, social media

ÚVOD

Účelom tohto príspevku je informovať čitateľov o rôznych technológiách a možných forenzných nástrojov v spojitosti odhaľovania extrémizmu.

Mobilné zariadenia, ako sú smartfóny a tablety, sa v 21. storočí stali neoddeliteľnou súčasťou každodenného života. Tieto zariadenia sú stálymi spoločníkmi a poskytujú rôzne pokročilé funkcie, ktoré umožňujú koncovým používateľom vykonávať širokú škálu činností. Príklady takýchto schopností zahŕňajú bezplatné komunikačné mechanizmy (napr. Wi-Fi, Bluetooth a Near Field Communication), vylepšené multimediálne funkcie (napr. nahrávanie videa, prehrávanie hudby a vysokokvalitné zobrazenie) a možnosť sťahovania ďalších aplikácií s pridanou funkcionalitou. Tieto schopnosti sú priamym výsledkom neustále sa zdokonaľujúcich hardvérových komponentov a vývoja mobilných operačných systémov.

Spoliehanie sa na mobilné zariadenia a ich všadeprítomné používanie koncovými používateľmi v spojení s ich neustále sa zvyšujúcou úložnou kapacitou umožňujú veľké množstvo digitálnych dát ukladať do interných a externých úložných priestorov. Takéto digitálne údaje zahŕňajú kontakty, textové a okamžité správy, históriu hovorov, geografické údaje, elektronickú poštu, históriu prehliadania webu a multimediálne aktivity. Dôkazná hodnota, ktorú ponúkajú takéto tradičné zdroje digitálnych údajov, sa stáva čoraz dôležitejšou, keď sú mobilné zariadenia súčasťou kriminálnych alebo nelegálnych aktivít. Tradičné zdroje digitálnych údajov môžu pomôcť digitálnym forenzným profesionálom, jednotlivcom zodpovedným za získavanie, zhromažďovanie, uchovávanie a analýzu digitálnych údajov získaných z mobilných zariadení, vytvárať hypotézy a odpovedať na kľúčové otázky počas vyšetrovania.

1 VYUŽÍVANIE DIGITÁLNYCH STÔP NA MOBILNÝCH ZARIADENICH V ZAHRANIČÍ

Extrémizmus možno definovať ako formu politickej aktivity, ktorá odmieta formy parlamentnej demokracie a zakladá svoju ideológiu a aktivity na neznášanlivosti, vylučovaní, xenofóbii a ultranacionalizme. Teda sa jedná o neznášanlivý prejav skupiny alebo jednotlivca sledujúci politické ciele. Extrémisti často pri nasledovaní svojich cieľov neberú ohľad či sa ich aktivity dotikajú civilného obyvateľstva. Často sa snažia zburcovať masy a to aj za cenu obetí. Vzhľadom ku skutočnosti, že smartfóny sú v spoločnosti veľmi populárne, a to tak u jednotlivcov, ako aj v podnikateľskom prostredí, ich používanie je vo veľkej časti využívané k uľahčeniu extrémistických aktivít, a to vrátane financovania extrémizmu.

Ukážkovým príkladom v spojení s potenciálne hroziacimi problémami takéhoto expertízneho skúmania digitálnych stôp uložených v mobilných zariadeniach (ďalej len MZ) pri vyšetrovaní extrémizmu je problematika okolo ich získavania. Teda problém súvisiaci nie tak so samotným zaistením MZ, na ktorom majú byť uložené potrebné informácie, ale samotné získanie informácii z daného MZ. Príklady upozorňujúce nás na hroziace ťažkosti, z ktorých sa môžeme učiť a ukazujúce nám aj spôsoby riešenia vznikajúcich problémov nachádzame často v zahraničí, ktoré je v technologickej oblasti vo vývoji často krát niekoľko rokov pred nami. Paralelne k zberu informácii mal Federálny úrad pre vyšetrovanie (FBI) pri získavaní spolupráce od spoločnosti Apple Inc. s cieľom odomknúť šifrovaný iPhone 5C problémy. Vyšetrovatelia v tomto prípade mali indície, ktoré napovedali, že predmetné MZ patrilo jednému z kľúčových podozrivých, avšak podozrivý niekoľko týždňov pred incidentom deaktivoval zálohovanie v službe poskytovateľa s názvom iCloud. Problémy vyplývajúce z tohto konkrétneho prípadu predstavujú potenciálne smerovanie kriminalistického skúmania digitálnych stôp z MZ v priamej súvislosti s ich využívaním pri extrémistických aktivitách, ako aj iných trestných činoch vo všeobecnosti.

Skúmanie a analýza informácii z mobilných cloudových služieb alebo mobilných komunikačných kanálov, vrátane komunikačných aplikácii (ako Viber, WhatsApp, messenger, a pod.) a e-mailov (Gmail, Outlook, a pod.) môže poskytnúť užitočné informácie pri rekonštrukcii extrémistických aktivít. Tieto informácie následne nadobúdajú dôležitosť nie len pre proces vyšetrovania ale aj pre samotné trestné konanie. Informácie ako záznamy z chatu, multimediálne súbory, zoznamy kontaktov a dáta o polohe, je možné použiť na určenie následnosti reťazca udalostí a na identifikáciu extrémistov a ich spolupracovníkov.

Aplikácie využívajúce cloudové úložisko sa pravidelne používajú na zabezpečenie synchronizácie (a to kvôli rýchlejšiemu prístupu k zoznamu kontaktov uložených na MZ, ktoré sa stanú prístupne aj napr. na tablete) a zdieľanie súborov. Bežne sa taktiež využívajú na automatické zálohovanie používateľského zariadenia (aby sa tak predišlo strate informácii v prípade zlyhania zariadenia a ľahšie sa preniesli na zariadenie nové). Napríklad služba Android Backup Service používa na zálohovanie používateľských údajov účty Google (napr. Google Drive, Google Photos). Výsledkom potom je, že postup potenciálne zanecháva dôkazné údaje, tak v zariadení používateľa cloudu, ako aj na cloudovom úložisku poskytovateľa služby. Tento postup vyžaduje teda odchýlky oproti klasickému modelu, prípadne zavedenie nových prístupov v procese zhromažďovania digitálnych stôp uložených na MZ. V ďalšom texte poukážem na možné spôsoby využitia kriminalistických postupov na vedenie vyšetrovania s ohľadom na získavanie digitálnych stôp. Postup pozostáva z nasledujúcich fáz:

i. Príprava a kriminalistická pripravenosť: Príprava premietnutá v rámci stratégii a nástrojov.
ii. Identifikácia: Táto fáza začína po zistení a nahlásení podozrivej udalosti.

iii. Hodnotenie, kriminalistický zber a analýza: Počiatočné hodnotenie sa vykonáva s cieľom rozhodnúť o rozsahu kriminalistickej analýzy a použitia vhodných zodpovedajúcich krokov.
iv. Konanie a monitorovanie: Zahŕňa konanie zamerané na potláčanie a elimináciu kybernetických bezpečnostných aktivít.
v. Obnova: Zahŕňa obnovu systémového narušenia do normálneho a zabezpečeného stavu.
vi. Vyhodnotenie a kriminalistické zhodnotenie: Prezentácia zistení a odporúčaní (Rahman, 2015).

Pretože sa MZ naďalej stávajú čoraz viac neoddeliteľnou súčasťou všetkých aspektov spoločnosti, je možné predpokladať, že sa naďalej bude zvyšovať dôležitosť kladená na vyšetrovanie v tejto oblasti digitálnych stôp. Vierohodnosť tejto pretrvávajúcej eskalácie spojená s rastúcimi právnymi dôsledkami vedie k preskúmaniu informačných a komunikačných technológii (IKTpočítačových zariadení z hľadiska ich využiteľnosti pri extrémistických trestných činoch. To nás privádza k potrebe zaoberať sa v akom rozsahu sa venuje pozornosť výskumným činnostiam v rámci kriminalistického skúmaní digitálnych stôp uložených na MZ.

1.1 KRÁTKY PRIEREZ V SKÚMANÍ MOBILNÝCH ZARIADENÍ V ZAHRANIČNEJ LITERATÚRE

Pri skúmaní metód zberu informácii Tassone (Tassone, Martini, Choo, Slay, 2013) demonštroval, že kriminalistické nástroje využívane v rámci skúmania digitálnych stôp uložených v MZ vyžadujú v závislosti od mobilného OS odlišné postupy. Tassoneho výskum naznačuje, že množstvo získaných digitálnych stôp sa líši s ohľadom na skúmaný OS a upozorňuje, že špecifické nástroje využívané pri fyzickom zbere informácii nemusia byť vždy k dispozícii. Dostupnosť týchto nástrojov vo veľkej miere závisia od modelu telefónu. To je v súlade so štúdiou Glissona (Glisson, Storer, Buchanan-Wollaston, 2013), ktorá dospela k záveru, že vo výsledkoch obnovy existujú značné rozdiely medzi metódami obnovy a medzi dostupnými nástrojmi. Vo výsledku berú na vedomie, že predmetnú odchýlku môžu spôsobovať výrobcovia, ktorí majú v rámci návrhov MZ celkovo rozličné požiadavky na dizajn, a teda aj softwarové vybavenie, a tomu zodpovedajú praktické odlišné technické rozhodnutia pri ich zostavovaní. Ďalej poukazuje na skutočnosť, že táto odlišnosť sťažuje overovanie informácii získaných rôznymi postupmi a nástrojmi. Jedna štúdia zameraná na zariadenia využívajúce Windows Phone, zdôrazňuje niekoľko vznikajúcich problémov pri zbere dát na troch telefónoch s týmto OS. Štúdia bola zameraná na neobnovené vymazané kontakty a správy v rámci procesu ich fyzického zberu a vplyvu reštartovania MZ na výsledok zberu informácii.

Zavedenie špecifických postupov a techník pri využívaní digitálnych stôp v procese vyšetrovania ma za cieľ zaistiť, že dôkazy je možné získať kriminalisticky spoľahlivým spôsobom. Chung (Chung, Park, Lee, Kang, 2012) poukazuje na prípadové štúdie ohľadne vybraných služieb cloudového úložiska, ako sú Amazon S3, Dropbox, Evernote a Google Docs, Chuang využil zálohové súbory iPhone-u a rootované zariadenie so systémom Android aby zhromaždil sledované stopy. Na základe McKemmishovho rámca Martini (Martini, Do, Choo, 2015) navrhol metodiku zhromažďovania a analýzy digitálnych stôp pre zariadenia Android s podrobnými procesmi vo fáze zhromažďovania informácii. Ariffin (Ariffin, D'Oorazio, Choo, Slay, 2013) v nadväznosti na predchádzajúce výskumy predstavil operačnú techniku na obnovenie odstránených obrazových súborov preskúmaním systémových súborov (denníkov) pre systém iOS. S tým ďalej súvisel aj výskum Leoma (Leoma, DOrazio, Deegan, Choo, 2015), ktorý preukázal, že kriminalistický zber a analýza miniatúr (v priečinku

.thumbnails) v OS Android majú signifikantný potenciál pre vyšetrovanie z pohľadu skúmania steganografie snímkou.

Posledný výskum Bermana a McMillana (McMillan, Glisson, Bromby, 2013) naznačuje, že využívanie digitálnych stôp o informáciách z GPS a MZ sa zvyšuje a ovplyvňuje samotný výsledok súdneho konania ako procesný dôkaz (v podmienkach slovenskej republiky by ekvivalentne ovplyvňoval už samotný proces vyšetrovania). Preto je právny význam z hľadiska dôkaznej hodnoty vo všeobecnosti založený na schopnosti vyhľadávať a získavať zvyškové údaje uložené na MZ právom stanoveným spôsobom.

Relevantnosť a prípustnosť zvyškových údajov závisí od hĺbkovej analýzy extrahovaných informácii. Analýza mobilných cloudových aplikácii vykonaných Martinim (Martini, Do, Choo, 2013) na Androide, a analýza vykonaná Grisposom (Grispos, Glisson, Storer, 2015) na iOS a Androide upozornila na rozdielnosť ukladania objektovo zhodných informácii v súborovom systéme zariadenia (teda na rozdiel ukladania tej istej informácie vzhľadom na použitý OS). Výskum, ktorý v nadväznosti na to podnikol Al Mutawa (Al Mutawa, Baggili, Marrington, 2012) ukázal rôzne výsledky extrakcie informácii z aplikácii súvisiacich so sociálnymi médiami, ako sú napr. Facebook, Twiter a MySpace. Stopy po aktivitách v sociálnych sieťach, ktoré sa nachádzali na zariadeniach Blackberry nebolo možné obnoviť, zatiaľ čo telefóny iPhone a Android uchovávali značné množstvo dôkazných údajov. Farhood (Farhood, Dehghantanha, Eterovic-Soric, Choo, 2015) vo svojom výskume následne podnikol experiment a preskúmal informácie v aplikáciách sociálnych médií, ktoré zostali vo vnútornej pamäti systému Android a vo vnútornom úložisku systému iOS, a ktoré poskytli digitálne stopy v podobe údajov o prihlásení, užívateľských mien, hesiel, mien, kontaktných informácii, profilových obrázkov, práce a vzdelania, polohu, zoznam priateľov, príspevky, správy, komentáre a IP adresy.

Anglano (Anglano, 2014) sa zameral hlavne na hĺbkovú analýzu informácii zanechaných programom WhatsApp Messenger a demonštroval, ako interpretovať údaje uložené v databázach kontaktov a chatov, aby tak mohli zostaviť zoznam kontaktov a chronológiu správ, ktoré boli zmenené používateľom. Ďalšia štúdia zdôraznila hĺbkovú analýzu s cieľom vytvoriť taxonómiu informácii. Azfar (Azfar, Choo, Liu, 2015) preskúmal 40 populárnych aplikácii Android mHealth a navrhol forenznú taxonómiu, ktorá obsahuje databázy, prihlasovacie údaje používateľov, osobné údaje používateľov, aktivity používateľov, polohu používateľov, časové značky aktivít a obrázky.

Sgaras (Sgaras, Kechadi, Le-Khac, 2015) analyzoval WhatsApp, Viber a Skype na zariadeniach so systémom android a iOS, ktoré produkovali cieľové informácie, ako sú údaje o inštalácii, prenášané údaje, údaje o obsahu, údaje používateľského profilu, údaje o autentifikácii používateľa, prílohy alebo vymieňané súbory, a údaje o polohe. Väčšina štúdii bola zameraná na simulovanie bežných aktivít používateľov pre konkrétne aplikácie a na preskúmanie ich využitia v trestnoprávnej rovine. Glisson (Glisson, Storer, Buchanan-Wollaston, 2013) sa zameral na získanie reálnych zariadení z trhu, ktoré sa predávali ako použité MZ a vykonal pokus s cieľom napodobniť situácie, ktorým by v reálnom živote čelili kriminalistický technici pri obnove údajov z neznámeho MZ. Vykonávanie bežných aktivít prostredníctvom aplikácii sociálnych médií, ako napríklad prihlasovanie sa do aplikácie, úprava osobných údajov, nahrávanie príspevkov, nahrávanie fotografií, uverejňovanie komentárov, posielanie e-mailov a chatovanie, podporuje skutočné porozumenie kriminalisticky relevantných informácii, ktoré sú generované týmito činnosťami.

2 EXTRÉMIZMUS A VYUŽÍVANIE MOBILNÝCH ZARIADENÍ

Pokiaľ ide o extrémizmus je dôležité pochopiť všetky aktivity, ktoré s ním súvisia, a samotný vplyv nových rozvíjajúcich sa (informačno komunikačných technológii) IKT, ako napríklad mobilná výpočtová technika. Aktivity súvisiace s extrémizmom možno rozdeliť zhruba nasledovne:

1) šírenie informácii,
2) utajovanie informácii,
3) získavanie finančných prostriedkov,
4) a nábor a zaúčanie (Rahman, 2015).

Šírenie informácii sa týka vytvárania a šírenia politicky alebo ideologicky motivovanej propagandy s cieľom ovplyvniť konkrétne publikum/komunity, radikalizovať potenciálnych podporovateľov a nabádať naivných jednotlivcov k extrémistickým a k iným trestným činom. Na šírenie sa používajú multimediálne objekty (ako napríklad videá a audio nahrávky), a to najčastejšie za využitia služieb sociálnych médií, ako sú webové stránky sociálnych sieti, on-line fóra, on-line hry, stránky slúžiace na zdieľanie videí a stránky poskytujúce priestor na zdieľanie súborov.

Utajovanie informácii spočíva v zneužívaní (zabezpečených) komunikačných platforiem na šírenie informácii s cieľom obísť kontrolu presadzovania práva a existujúce nástroje dohľadu. Metóda využívajúca sa na utajovanie správ sa nazýva steganografia. Stenograficka metóda využíva úpravu najmenej nápadného bitu na ukrytie správy do digitálneho objektu, ako je napríklad textový súbor, obrázok alebo zvuk. Za pomoci pokroku v možnostiach MZ, ako aj s dostupnosťou voľne šíriteľných softwearov využívajúcich steganografickú metódu, je veľmi jednoduché ukryť skutočnú správu v takýchto zariadeniach. Podobné zahmlievanie správ sťažuje identifikáciu a sledovanie nelegálnej komunikácie týkajúcej sa extrémistických aktivít a finančných transakcii.

Získavanie finančných prostriedkov predstavuje zhromažďovanie finančných prostriedkov na podporu extrémizmu, a s tým súvisiacich operácii. Zdroje financovania zahŕňajú dary od podporovateľov, presmerovanie finančných prostriedkov získaných legitímnymi prostriedkami (charitatívne dary) a výnosy z trestnej činnosti. Takáto zbierka by pochádzala z viacerých zdrojov, ako sú napríklad dary od podporovateľov, z prania špinavých peňazí od charitatívnych organizácii, ktoré by však boli zneužité na teroristické účely a nelegálnu činnosť. Nábor členov extrémistických skupín zahŕňa oslovenie, komunikáciu, ovplyvňovanie a radikalizáciu rovnako zmýšľajúcich osôb využitím IKT (napr. stránky sociálnych sieti).

S ľahkosťou akou sa v súčasnosti šíria a uchovávajú informácie na MZ a v spojení s dostupnosťou aplikácii na utajovanie alebo skrytie správ, sa priamoúmerne zvyšuje efektivita financovania extrémizmu a rovnako aj náboru nových členov. Preto je cieľom tohto článku zamerať sa na identifikáciu informácii, ktoré sú zanechávané v MZ po ich použití v súvislosti s činnosťami, ktoré súvisia so šírením a skrývaním informácii.

3 MOBILNÉ ZARIADENIA AKO NOSIČE DIGITÁLNYCH STÔP

Pokiaľ sa v rámci kriminalistiky zaoberáme digitálnymi stopami a konkrétnejšie informáciami uloženými na MZ, je potrebné brať ohľad na zber údajov, ktorý zahŕňa fyzické, logické a manuálne metódy (Rahman, 2015). Získavanie informácii fyzickými metódami je priamo spojené s obnovením binárnych zobrazení vnútornej pamäte MZ a ich ukladaním do samostatných súborov pre ďalšie využitie. Na druhej strane logické metódy slúžia na získavanie informácii, ktoré sú priamo späté s operačným systémom (ďalej len OS) MZ a obnovujú logické okruhy uložené v súborovom systéme. Manuálne metódy zahrnujú

prezeranie dátového obsahu uloženého v MZ, ktoré si vyžaduje manuálnu manipuláciu s tlačidlami, klávesnicou alebo dotykovou obrazovkou a ktoré je možné zaznamenávať pomocou externého digitálneho fotoaparátu.

Kriminalistický výskum s ohľadom na digitálne stopy spojené s MZ možno v jednoduchosti rozdeliť na:

1) výber správnej metódy zberu informácii,
2) uskutočňovanie podrobných kriminalistických postupov,
3) a vykonanie hĺbkovej kriminalistickej analýzy aplikácii uložených v MZ alebo v OS MZ.

3.1 DIGITÁLNE STOPY A MIESTO TRESTNÉHO ČINU

Z tohto pohľadu sú pre nás podstatné predovšetkým prostriedky výpočtovej, telekomunikačnej, záznamovej techniky a ďalšie techniky, uchovávajúce digitálne záznamy, ktoré sa na miestach trestných činov vyskytujú buď to priamo alebo sprostredkovane (mobilné zariadenie s dôležitými informáciami by páchateľ, prípadne niekto iný mohol odniesť alebo zničiť. Môže však dôjsť aj k tomu, že za pomoci mobilného zariadenia by na mieste trestného činu mohol páchateľ komunikovať so vzdialenými počítačmi, aplikáciami alebo aj vozidlom, ktoré má zabudovaný navigačný systémom, a ktoré mohol páchateľ využiť pri úteku z miesta trestného činu a pod.). Digitálne stopy bývajú mnohokrát v praxi podceňované, a to tak vzhľadom na ich význam, obsažnosť, spôsob zabezpečenia a následnú analýzu. Podstatnú úlohu v tejto oblasti zohrávajú nielen špecializované forenzné laboratória či ústavy, ale hlavne tie zložky vyšetrovacích orgánov, ktoré sa na miestach trestných činov objavujú ako prvé, alebo ktoré vedú bezprostredné následne vyšetrovanie. Bez toho aby tieto osoby mali dostatočné odborné znalosti v tejto prvotnej fázy vyšetrovania nemôže byť vyšetrovanie nikdy úspešné. Na tomto mieste treba konštatovať, že nemáme na mysli odborné znalosti IKT prostriedkov, ale ide skôr o organizačné a metodické postupy, u ktorých je potreba garancie včasného zabezpečenia kvalitných digitálnych stôp a možností zabránenia ich znehodnotenia či zneužitia. Vyžaduje sa teda spolupráca s ďalšími špecializovanými útvarmi.

Pokiaľ ide o miesto trestného činu v prípade digitálnych stôp môže dôjsť k ťažkostiam, a teda môže byť za určitých okolnosti veľmi ťažko geograficky určené. Na druhú stranu pokiaľ ide o samostatné zariadenie (mobilné zariadenie, fotoaparát, videokamera, personálny asistent (PDA), atď.), od siete oddelený PC alebo notebook na ktorom sú uložené dôkazy je situácia pomerne jednoduchá. V takomto prípade sú digitálne stopy uložené priamo v daných zariadeniach alebo dátových nosičoch s nimi kompatibilnými.

O zložitejšiu situáciu pôjde keď počítač je pripojený do podnikovej siete, do prostredia internetu a ak má užívateľ prístup k väčšiemu množstvu najrôznejších aplikácii, serverov, zariadení a pod. Serveri častokrát nemusia byť uložené priamo v danej inštitúcii. Častokrát sú v krajinách na druhej strane sveta. Nie je pochýb, že páchatelia, ktorí využívajú tieto technológie na šírenie svojich myšlienok a porušovanie zákona prostredníctvom počítačovej alebo kybernetickej kriminality si veľmi dobre uvedomujú význam digitálnych stôp, a že pre nich predstavujú mimoriadne riziko. Ich činnosť teda smeruje k pokusom o skrytie týchto stôp a tým sa snažia zviesť vyšetrovanie iným smerom, prípadne sa pokúšaju vyšetrovateľa zahltiť nesmiernym množstvom falošných, ťažko overiteľných informácii. Za týmto účelom sú schopný použiť viaceré metódy ako – krádež identity iného užívateľa (túto identitu ďalej využívajú a pod ktorým užívateľským kontom potom ďalej vystupujú). Ďalej sa napríklad snažia o ovládnutie najvyšších administrátorských práv správcu systému. Tieto metódy im v maximálnej miere dovoľujú zahladzovať stopy a v digitálnom prostredí sa pohybovať takmer neviditeľne. Útoky na servery sa spravidla nevykonávajú priamo, ale postupným, niekoľkonásobným, reťazovým ovládnutím väčšieho počtu serverov. To má za následok, že

poškodený nevie, kto je páchateľom útoku. Vyšetrovateľom celé vyšetrovanie sťažuje aj to, že musia nájsť celý reťazec týchto krokov páchateľa. Aby sa dopátrali až na koniec reťazca potrebujú vyšetrovatelia vedieť, čo hľadať a taktiež sa pokúsiť zabezpečiť všetky relevantné digitálne stopy podporujúce dané vyšetrovacie verzie s dostatočnou kvalitou dôkazného materiálu. Ako už bolo vyššie spomenuté, geografické určenie miesta trestného činu je v takomto prípade oveľa ťažšie identifikovateľné, než pokiaľ ide o klasické trestné činy, pre ktoré sú charakteristické mechanické, biologické, daktyloskopické, traseologické, balistické, pyrotechnické a ďalšie druhy stôp, ohraničené na malom fyzickom priestore. Problematická u digitálnych stôp je predovšetkým skutočnosť, že sa často jedná o veľké množstvo fyzicky veľmi malých zariadení, ktoré sú podmienené práve veľkosťou toho ktorého nosiča informácie, a ktoré od seba môže oddeľovať obrovská vzdialenosť. Celú situáciu komplikuje aj to, že na prvý pohľad nemusí byť samotné prepojenie medzi týmito dôkaznými nosičmi zjavné.

Sledovanie digitálnych stôp sťažuje a ich potenciálne veľká pravdepodobnosť kombinácii s rôznymi technológiami, ktorú umocňuje zapojenie väčšieho množstva páchateľov. Účelom je ich deľba činnosť, respektíve zdieľanie spoločných prostriedkov alebo poznatkov. Takýmto spôsobom dokážu pôsobiť z viacerých miest. Rovnako aj digitálne stopy môžu byť výsledkom organizovanej trestnej činnosti. V takomto prípade tu môžu mimo páchateľov vystupovať aj nastrčené, nič netušiace osoby.

Globálna oblasť extrémistických trestných činov môže byť mnohokrát veľmi zložitá, členitá a rozsiahla. Je preto potrebné vyčleniť typické oblasti, kde je nutné hľadať digitálne stopy. Fáza vyhľadávania digitálnych stôp je rozdelená do štyroch oblastí (Porada, Straus, 2012).

Oblasť záujmu – podstatný je cieľ útoku, kde páchateľ realizuje svoje požiadavky, ciele a záujmy.

Potom **oblasť podpory záujmu** – ide o okolité prostredie, ktoré bezprostredne hraničí s oblasťou záujmu. Ide napríklad o servery na prístupových trasách, rôzne komunikačné siete, spolupáchatelia, nastrčené osoby, a pod. Táto oblasť často krát vystupuje ako krycie prostredie, ktorého cieľom je získať legendu pre nelegálnu činnosť, alebo zahladiť a zničiť digitálne stopy vedúce k páchateľovi. Na druhú stranu môže niekedy vystupovať aj ako skutočný prostriedok na realizáciu trestného činu.

Ďalšou je **oblasť páchateľa** – ide o miesto, na ktorom sú páchateľom realizované aktivity trestného činu. Odtiaľto môžu viesť digitálne stopy k spolupáchateľom alebo technologickým prostriedkom akými sú napríklad mobilné zariadenia. Zaistenie digitálnych stôp môže mať častokrát za následok odhalenie celej organizačnej štruktúry. Z tohto dôvodu predstavuje oblasť páchateľa rovnako veľmi dôležitú súčasť celého procesu vyhľadávania digitálnych stôp.

Poslednou je oblasť **zázemia páchateľa** – v prípade dlhodobo plánovaných trestných činov páchateľ zvyčajne zvažuje kam skryť buď hodnoty získane trestným činom alebo technické nosiče preukazujúce jeho vinu. Bezprostredná oblasť páchateľa častokrát nezabezpečuje dostatočné bezpečie v prípade, ak dôjde na vyšetrovanie. Ide o ďalší z možností skrývania úspešnej trestnej činnosti. Jej cieľ predstavuje snaha o prerušenie všetkých logických ako aj fyzických väzieb medzi páchateľom a výsledkom jeho činnosti. Informácie, ktoré získal môže uložiť na vopred pripravené miesto, ktoré je osobité svojou štruktúrou, formátom dátového média a pod. Na tento účel nie je možné vylúčiť ani napríklad trezor v banke, kde sa dajú uskladniť tak peniaze ako aj dátové nosiče a pod. Ako správca môže opäť figurovať aj ďalší spolupracovník. Tento spolupracovník môže vopred vedieť alebo naopak nemusí ani tušiť, čo spravuje a chráni pred „ nepovolanými“ osobami. Pod túto oblasť možno subsumovať „korisť“ z trestného činu alebo taktiež môže poskytovať kľúčové

informácie k jej nájdeniu. Všetky oblasti spája skutočnosť, že bývajú zväčša dlhodobo alebo krátkodobo digitálne prepojené, a tým pádom vytvárajú množstvo digitálnych stôp.

3.2 FORENZNÉ NÁSTROJE

Dostupnosť forenzných softvérových nástrojov pre mobilné zariadenia sa značne líši od dostupnosti osobných počítačov. Aj keď sa osobné počítače môžu líšiť od mobilných zariadení z hľadiska hardvéru a softvéru, ich funkčnosť je čoraz podobnejšia. Väčšina operačných systémov mobilných zariadení je open source (t. j. Android). Uzavreté operačné systémy sťažujú interpretáciu ich pridruženého súborového systému a štruktúry. Mnoho mobilných zariadení s rovnakým operačným systémom sa tiež môže značne líšiť v implementácii, čo vedie k nespočetnému množstvu permutácií súborových systémov a štruktúr. Tieto permutácie predstavujú významné výzvy pre výrobcov mobilných forenzných nástrojov.

Typy softvéru dostupného na preskúmanie mobilných zariadení zahŕňajú komerčné forenzné nástroje a forenzné nástroje s otvoreným zdrojom, ako aj neforenzné nástroje určené na správu, testovanie a diagnostiku zariadení. Forenzné nástroje sú zvyčajne navrhnuté tak, aby získavali údaje z internej pamäte mobilných telefónov a UICC bez toho, aby menili ich obsah, a na výpočet hodnôt haš integrity získaných údajov. Forenzné aj neforenzné softvérové nástroje často používajú rovnaké protokoly a techniky na komunikáciu so zariadením. Neforenzné nástroje však môžu umožniť neobmedzený obojsmerný tok informácií a vynechať hašovacie funkcie integrity údajov. Osoby zaoberajúce sa vyšetrovaním mobilných zariadení zvyčajne zostavujú kolekciu forenzných aj neforenzných nástrojov. Rozsah zariadení, na ktorých fungujú, je zvyčajne zúžený na: odlišné platformy, špecifickú rodinu operačných systémov alebo dokonca jeden typ hardvérovej architektúry. Rýchla výroba a rôznorodosť sú normou pre MZ a vyžaduje, aby výrobcovia nástrojov neustále aktualizovali svoje nástroje a poskytli forenzným expertom forenzné riešenia. Táto úloha je náročná a podpora vývojárov nástrojov pre novšie modely môže výrazne zaostávať za uvedením zariadenia na trh. Modely starších funkčných mobilných zariadení, aj keď sú zastarané, sa môžu používať aj roky po ich prvom uvedení na trh. Modely mobilných zariadení uvedené na jeden vnútroštátny trh sa môžu používať aj v oblastiach výmenou UICC jedného mobilného operátora za UICC iného operátora. Súčasný stav bude pravdepodobne pokračovať, pričom náklady na vyšetrenie budú výrazne vyššie, ako keby prevládalo niekoľko štandardných operačných systémov a hardvérových konfigurácií.

3.3 SYSTÉM KLASIFIKÁCIE NÁSTROJOV MOBILNÝCH ZARIADENÍ

Pre mobilného forenzného experta je dôležité porozumieť rôznym typom mobilných nástrojov na obnovu údajov. V tejto rovine rozoznávame viaceré metódy

Metódy manuálnej extrakcie zahŕňajú zaznamenávanie informácií zobrazených na obrazovke mobilného zariadenia pri použití používateľského rozhrania. Metódy logickej extrakcie sa v súčasnosti používajú najčastejšie a sú mierne technické, vyžadujúce školenie na úrovni začiatočníkov. Ďalšie metódy zahŕňajú extrahovanie a zaznamenávanie kópie alebo obrazu fyzického úložiska (napr. pamäťového čipu), v porovnaní s logickými metódami zahŕňajú zachytenie kópie objektov logického úložiska (napr. adresárov a súborov), ktoré sa nachádzajú v logickom úložisku (napr. oddiel systému súborov). Ďalej poznáme metódy Hex Dumping/JTAG extrakcie, zahŕňajú vykonávanie „fyzického zberu informácii “ z pamäte mobilného zariadenia. Metódy Chip-Off zahŕňajú fyzické odstránenie pamäte z mobilného zariadenia na extrahovanie údajov, čo si vyžaduje rozsiahle školenie v oblasti elektronického inžinierstva a forenznej analýzy súborových systémov. Metódy Micro Read zahŕňajú použitie

vysokovýkonného mikroskopu na zobrazenie fyzického stavu brán. Ide o najinvazívnejšiu, najsofistikovanejšiu, najtechnickejšiu, najdrahšiu a časovo najnáročnejšiu zo všetkých metodík.

Vykonávanie týchto typov extrakcie má svoje výhody a nevýhody. Napríklad hex dumping umožňuje preskúmať vymazané objekty a akékoľvek prítomné zvyšky údajov (napr. v nepridelenej pamäti alebo priestore súborového systému), ktoré by inak boli nedostupné pomocou metód logického získavania. Extrahované obrázky zariadenia však vyžadujú analýzu, dešifrovanie a dekódovanie. Logické metódy získavania, aj keď sú obmedzenejšie ako metódy Hex Dumping/JTAG, majú výhodu v tom, že systémové dátové štruktúry sú na vyššej úrovni abstrakcie. Tieto rozdiely sú spôsobené základným rozdielom medzi pamäťou, ako ju vidí proces prostredníctvom zariadení operačného systému (t. j. logický pohľad), a pamäťou, ako ju vidí v surovej forme procesor alebo iný hardvérový komponent (t. j. fyzický pohľad). Pri každej metodike môžu byť údaje natrvalo zničené alebo upravené, ak sa daný nástroj alebo postup nevyužíva správne. Správne školenie a mentoring sú preto rozhodujúce pre dosiahnutie najvyššej úspešnosti extrakcie údajov a analýzy údajov obsiahnutých v mobilných zariadeniach.

Nasledujúca diskusia poskytuje podrobnejší popis každej metódy používanej na extrakciu údajov.

- **Manuálna extrakcia** – Metóda manuálnej extrakcie zahŕňa prezeranie dátového obsahu uloženého v mobilnom zariadení. Obsah zobrazený na obrazovke LCD vyžaduje na zobrazenie obsahu mobilného zariadenia manuálnu manipuláciu s tlačidlami, klávesnicou alebo dotykovou obrazovkou. Zistené informácie možno zaznamenať pomocou externého digitálneho fotoaparátu. Na tejto úrovni nie je možné obnoviť odstránené informácie. Niektoré nástroje boli vyvinuté, aby poskytli forenznému vyšetrovateľovi schopnosť rýchlejšie dokumentovať a kategorizovať zaznamenané informácie. Napriek tomu, ak je potrebné zachytiť veľké množstvo údajov, manuálna extrakcia môže byť veľmi časovo náročná a údaje na zariadení môžu byť v dôsledku vyšetrenia neúmyselne zmenené, vymazané alebo prepísané. Manuálne extrakcia je čoraz ťažšia a možno aj nemožná, pokiaľ ide napr. o rozbitú/chýbajúcu LCD obrazovku alebo poškodené/chýbajúce rozhranie klávesnice. Ďalšie problémy sa vyskytujú, keď je zariadenie nakonfigurované tak, aby zobrazovalo jazyk, ktorý vyšetrovateľ nepozná; to môže spôsobiť ťažkosti pri úspešnej navigácii v zariadení.
- **Logická extrakcia** – Konektivita medzi mobilným zariadením a forenznou pracovnou stanicou sa dosiahne pripojením pomocou káblového (napr. USB alebo RS-232) alebo bezdrôtového (napr. IrDA, WiFi alebo Bluetooth) pripojenia. Vyšetrovateľ by si mal byť vedomý problémov spojených s výberom konkrétneho spôsobu pripojenia, pretože rôzne typy pripojenia a súvisiace protokoly môžu viesť k úprave údajov (napr. neprečítané SMS) alebo k extrahovaniu rôznych množstiev alebo typov údajov. Logické extrakčné nástroje začínajú odoslaním série príkazov cez zavedené rozhranie z počítača do mobilného zariadenia. Mobilné zariadenie odpovie na základe príkazu. Odpoveď (údaje mobilného zariadenia) sa odošle späť na pracovnú stanicu a predloží sa forenznému vyšetrovateľovi na účely správy.
- **Hex Dumping a JTAG** – Hex Dumping a metódy extrakcie JTAG (Joint Test Action Group) umožňujú forenznému vyšetrovateľovi priamejší prístup k nespracovaným informáciám uloženým v pamäti. Jednou z výziev týchto metód extrakcie je schopnosť daného nástroja analyzovať a dekódovať zachytené údaje. Poskytnúť forenznému vyšetrovateľovi logický pohľad v systéme súborov. Problém môže nastať napríklad, keď nemusia byť získané všetky dáta obsiahnuté v danom flash pamäťovom čipe, pretože mnohé nástroje, ako napríklad flash boxy, môžu byť schopné extrahovať iba

špecifické časti pamäte. Tieto metódy vyžadujú konektivitu (napr. kábel alebo WiFi) medzi mobilným zariadením a forenznou pracovnou stanicou.

- **Hex Dumping** – táto technika je najčastejšie používanou metódou nástrojov. Ide o nahranie upraveného zavádzača (alebo iného softvéru) do chránenej oblasti pamäte (napr. RAM) v zariadení. Tento proces nahrávania sa dosiahne pripojením dátového portu mobilného zariadenia k flasher box-u a flasher box je zase pripojený k forenznej pracovnej stanici. Séria príkazov sa odošle z flasher boxu do mobilného zariadenia, aby sa preniesli do diagnostického režimu. Keď je flasher box v diagnostickom režime, zachytí celú (alebo časti) pamäte a odošle ju do forenznej pracovnej stanice cez rovnaké komunikačné prepojenie, aké sa používa na nahrávanie. Niektoré flasher boxy fungujú týmto spôsobom alebo môžu používať proprietárne rozhranie na extrakciu pamäte. Existujú zriedkavé prípady, keď je možné extrakciu vykonať pomocou WiFi.
- **JTAG** – Mnoho výrobcov podporuje štandard JTAG, ktorý definuje spoločné testovacie rozhranie pre procesor, pamäť a ďalšie polovodičové čipy. Forenzní experti môžu komunikovať s komponentom kompatibilným s JTAG využitím špeciálnych samostatných programovacích zariadení na snímanie definovaných testovacích bodov. JTAG poskytuje špecialistom ďalšiu cestu pre zobrazovacie zariadenia, ktoré sú uzamknuté alebo zariadenia, ktoré môžu mať menšie poškodenie a nemôžu byť inak správne prepojené. Táto metóda zahŕňa pripojenie kábla (alebo káblového zväzku) z pracovnej stanice k rozhraniu JTAG mobilného zariadenia a prístup k pamäti cez mikroprocesor zariadenia na vytvorenie obrazu. Extrakcie JTAG sa líšia od Hex Dumpingu hlavne tým, že sú invazívne, pretože prístup k pripojeniam často vyžaduje, aby došlo k rozoberaniu mobilného zariadenia, kvôli získaniu prístupu na vytvorenie káblových spojení.

Flasher box pomáha vyšetrovateľovi pri komunikácii s mobilným zariadením pomocou diagnostických protokolov na komunikáciu s pamäťovým čipom. Táto komunikácia môže využívať operačný systém mobilného zariadenia alebo ho môže úplne obísť a komunikovať priamo s čipom. Flasher boxy sú často sprevádzané softvérom na uľahčenie procesu extrakcie dát, ktorý funguje v spojení s hardvérom. Mnoho softvérových balíkov poskytuje v niektorých konfiguráciách pridanú funkciu obnovy hesiel z pamäte mobilného zariadenia. Aj keď sa metódy získavania medzi flasher boxmi líšia, používa sa všeobecný proces. Obmedzenia používania flasher boxov zahŕňajú nasledujúce:

- Na začatie procesu extrakcie je často potrebné reštartovať mobilné zariadenie; to môže spôsobiť aktiváciu autentifikačných mechanizmov, ktoré zabránia ďalšej analýze.
- Mnohé flasher boxy obnovujú údaje v zašifrovanom formáte, ktorý vyžaduje, aby vyšetrovateľ buď použil softvér poskytnutý výrobcom boxu na dešifrovanie údajov, alebo môže vyžadovať spätné inžinierstvo šifrovacej schémy údajov zo strany analytika.
- Mnoho modelov telefónov neposkytuje získanie celého rozsahu pamäte v rámci daného mobilného zariadenia. Pre určité mobilné zariadenia môžu byť dostupné len určité rozsahy.
- Servisný softvér flasher boxu má často veľa tlačidiel, ktoré sú označené takmer identickými názvami. Tento zmätok môže ľahko viesť aj skúseného vyšetrovateľa k tomu, že stlačí nesprávne tlačidlo a vymaže obsah mobilného zariadenia namiesto vyprázdnenia pamäte.
- Bežný je nedostatok dokumentácie o používaní nástrojov flasher boxu. Metódy extrakcie sú často zdieľané na fórach podporovaných predajcom a moderované skúsenejšími používateľmi. Pri poskytovaní rád je potrebné postupovať opatrne, pretože nie všetky poskytnuté informácie sú správne.

- Forenzné použitie: Flasher boxy pôvodne neboli navrhnuté na forenzné použitie. Vyšetrovateľa musia mať skúsenosti s používaním flasher boxov a mali by rozumieť ich správnemu používaniu a funkcii.
- Napriek všetkým týmto obmedzeniam je použitie flasher boxu životaschopnou možnosťou pre mnohé forenzné prípady. Správne školenie, skúsenosti a pochopenie toho, ako nástroje fungujú, sú kľúčom k úspechu.

Na extrahovanie a analýzu binárnych obrazov pomocou týchto metód, vrátane lokalizácie a pripojenia k portom JTAG, vytvárania prispôsobených zavádzačov a opätovného vytvárania súborových systémov, je potrebná široká škála technických znalostí a riadne školenie.

- **Chip-Off** – metódy Chip-Off sa týkajú získavania údajov priamo z pamäte mobilného zariadenia. Táto extrakcia vyžaduje fyzické odstránenie pamäte. Chip-Off poskytuje vyšetrovateľovi možnosť vytvoriť binárny obraz odstráneného čipu. Aby sa vyšetrovateľovi poskytli údaje v súvislom súbore binárneho formátu, algoritmus vyrovnávania opotrebovania musí byť reverzne navrhnutý. Po dokončení môže byť binárny obraz analyzovaný. Tento typ akvizície je najužšie spojený s fyzickým zobrazovaním jednotky pevného disku ako v tradičnej digitálnej forenznej analýze. Na úspešné vykonávanie extrakcií na tejto úrovni je potrebný rozsiahly tréning. Extrakcie čipov sú náročné vzhľadom na širokú škálu typov čipov, nespočetné množstvo formátov nespracovaných údajov a riziko fyzického poškodenia čipu počas procesu extrakcie. Kvôli zložitostiam súvisiacim s Chip-Off je extrakcia JTAG bežnejšia.
- **Micro Read** – Micro Read zahŕňa zaznamenávanie fyzického pozorovania brán na čipe NAND alebo NOR pomocou elektrónového mikroskopu. Kvôli extrémnym technickým aspektom pri vykonávaní tejto metódy k nej pristupuje len v prípade závažných prípadov ekvivalentných kríze národnej bezpečnosti po vyčerpaní všetkých ostatných techník získavania. Úspešná akvizícia na tejto úrovni by si vyžadovala tím odborníkov, vhodné vybavenie, čas a hĺbkové znalosti chránených informácií. V súčasnosti neexistujú žiadne komerčne dostupné nástroje Micro Read.

3.4 NÁSTROJE UICC

Niekoľko mobilných forenzných nástrojov sa zaoberá výlučne UICC. Tieto nástroje vykonávajú priame čítanie obsahu UICC prostredníctvom čítačky osobných počítačov/inteligentných kariet (PC/SC), na rozdiel od nepriameho čítania cez mobilné zariadenie. Bohatosť a rozsah získaných údajov sa líši v závislosti od možností a funkcií nástroja. Väčšina exkluzívnych nástrojov UICC získava tieto údaje: Medzinárodná identita mobilného predplatiteľa (IMSI), ID karty integrovaného okruhu (ICCID), čísla skrátenej voľby (ADN), posledné volané čísla (LND), SMS správy a informácie o polohe (LOCI).

Väčšina nástrojov poskytuje ďalšie informácie, ako sú vymazané SMS správy, správne vykreslené cudzojazyčné SMS a EMS správy. Pokúšajú sa tiež preložiť určité údaje, ako sú kódy krajín a sieťových operátorov, do zmysluplných názvov a poskytnúť ďalšie možnosti, ako napríklad správu PIN.

Oddiely CSIM na UICC sa čoraz častejšie používajú pre mobilné zariadenia s podporou LTE. V súčasnosti len málo nástrojov podporuje extrakciu údajov oddielov CSIM, pretože väčšina podporuje iba extrahovanie oddielov GSM a USIM. Údaje CSIM môžu pribúdať forenzný význam, pretože táto technológia sa vyvíja.

3.5 ZABLOKOVANÉ ZARIADENIA

Nasledujúce časti pojednávajú o technikách na obídenie zablokovaného zariadenia, t. j. mobilného zariadenia, ktoré vyžaduje úspešné overenie pomocou hesla alebo iných prostriedkov na získanie prístupu k zariadeniu. Existuje niekoľko spôsobov, ako obnoviť údaje zo zablokovaných zariadení. Tieto metódy spadajú do jednej z troch kategórií: softvérové, hardvérové a vyšetrovacie. Medzi bežné zablokované zariadenia patria zariadenia s chýbajúcimi modulmi identity, kódmi UICC s povoleným kódom PIN alebo so zapnutým zámkom mobilného zariadenia. Pamäťové karty uzamknuté heslom a šifrované poskytujú používateľovi ďalšie prostriedky na ochranu údajov. Táto ochrana môže urobiť obnovu takýchto údajov zložitejšou. Možnosti šifrovania obsahu sú ponúkané ako štandardná funkcia v mnohých mobilných zariadeniach alebo môžu byť dostupné prostredníctvom doplnkových aplikácií. Softvérové a hardvérové metódy sú často zamerané na konkrétne zariadenie alebo úzku triedu zariadení.

Ako sa mobilné forenzné nástroje vyvíjali, začali poskytovať automatizované funkcie umožňujúce vyšetrovateľom obísť mnohé bezpečnostné mechanizmy ako súčasť ich produktov. Niektoré nástroje napríklad poskytujú automatizovanú funkciu na obnovenie hesiel z uzamknutých mobilných zariadení. Pri vývoji metódy poskytujú nasledujúce časti činnosti, ktoré by sa mali zvážiť pri určovaní možných prístupov.

3.5.1 SOFTVÉROVÉ A HARDVÉROVÉ METÓDY

Začali sa objavovať softvérové metódy používané na prelomenie alebo obídenie autentifikačných mechanizmov. Niektoré nástroje napríklad poskytujú automatizovanú funkciu na obnovenie hesiel z uzamknutých mobilných zariadení. Tento typ funkcionality sa medzi mobilnými forenznými nástrojmi a modelmi zariadení, ktoré sú podporované, značne líši.

Hardvérové metódy zahŕňajú kombináciu softvéru a hardvéru na prelomenie alebo obídenie autentifikačných mechanizmov a získanie prístupu k zariadeniu. Napríklad hodnotu zámku mobilného zariadenia možno ľahko obnoviť z výpisu pamäte určitých zariadení, čo umožňuje následné logické získavanie. JTAG a flasher boxy sa často používajú týmto spôsobom na obídenie autentifikačných mechanizmov. Na obídenie autentifikačných mechanizmov existujú útoky špecifické pre zariadenie, ako napríklad útoky za studena. Útoky za studena majú schopnosť obnoviť heslá z uzamknutých zariadení so systémom Android ochladením zariadenia na -10 stupňov Celzia, po ktorom nasleduje odpojenie a opätovné pripojenie batérie v intervaloch 500 ms.

Len málo univerzálnych hardvérových metód sa vzťahuje na všeobecnú triedu mobilných zariadení. Väčšina techník je prispôsobená pre konkrétny model v rámci triedy.

3.5.2 VYŠETROVACIE METÓDY

Vyšetrovacie metódy sú postupy, ktoré môže použiť vyšetrovací tím a ktoré nevyžadujú žiadne forenzné softvérové alebo hardvérové nástroje. Najzrejmejšie metódy sú nasledujúce:

- **Opýtajte sa majiteľa** – Ak je zariadenie chránené heslom, PIN kódom alebo iným autentifikačným mechanizmom, ktorý zahŕňa autentizáciu založenú na znalostiach, vlastník môže byť požiadaný o tieto informácie počas rozhovoru.
- **Skontrolujte zadržaný materiál** – Heslá alebo PIN kódy si môžete zapísať na kúsok papiera a uložiť ich s telefónom alebo v jeho blízkosti, v stolnom počítači používanom na synchronizáciu s mobilným zariadením alebo s vlastníkom, napríklad v peňaženke,

získané vizuálnou kontrolou. Obalový materiál pre UICC alebo mobilné zariadenie môže obsahovať PIN Unlocking Key (PUK), ktorý možno použiť na resetovanie hodnoty PIN. Môžu sa tiež využiť slabé miesta špecifické pre zariadenie, ako napríklad útoky Smudge.

- **Opýtajte sa poskytovateľa služieb** – Ak je mobilné zariadenie GSM chránené kódom UICC s povoleným PIN, možno od neho získať identifikátor (t. j. ICCID) a použiť ho na vyžiadanie PUK od poskytovateľa služieb a resetovanie PIN. Niektorí poskytovatelia služieb ponúkajú možnosť získať PUK online zadaním telefónneho čísla mobilného zariadenia a špecifických informácií o predplatiteľovi na verejných webových stránkach vytvorených na tento účel. Okrem toho môžete informácie získať kontaktovaním výrobcu zariadenia (napr. Apple).
- Používatelia mobilných zariadení si môžu na zabezpečenie svojho zariadenia zvoliť **slabé heslá**, ako napríklad: 1-1-1-1, 0-0-0-0 alebo 1-2-3-4. Niektoré z týchto číselných kombinácií sú predvolené prístupové kódy zariadenia poskytnuté výrobcom. Neodporúča sa pokúšať sa odomknúť zariadenie pomocou týchto kombinácií z dôvodu niekoľkých rizikových faktorov. Môžu zahŕňať trvalé vymazanie pamäte mobilného zariadenia, aktiváciu dodatočných bezpečnostných mechanizmov (napr. PIN/PUK) alebo inicializáciu deštruktívnych aplikácií. Mobilné zariadenia majú vo všeobecnosti definovaný počet pokusov, kým povolia ďalšie bezpečnostné opatrenia. Pred akýmkoľvek pokusom o odomknutie mobilného zariadenia sa odporúča zvážiť počet zostávajúcich pokusov. Môže nastať prípad, keď sa skúšajúci môže rozhodnúť akceptovať tieto riziká v prípadoch, keď je to jediná možnosť extrakcie údajov.

3.6 MOŽNOSTI FORENZNÝCH NÁSTROJOV

Forenzné softvérové nástroje sa snažia zvládnuť konvenčné vyšetrovacie potreby tým, že sa zaoberajú širokou škálou použiteľných zariadení. Zložitejšie situácie, ako je obnova vymazaných údajov z pamäte zariadenia, si môžu vyžadovať špecializovanejšie nástroje a odborné znalosti a demontáž zariadenia. Rozsah poskytovanej podpory vrátane káblov a ovládačov mobilných zariadení, dokumentácie k produktu, čítačiek PC/SC a frekvencie aktualizácií sa môže medzi jednotlivými produktmi výrazne líšiť. Ponúkané funkcie, ako je vyhľadávanie, vytváranie záložiek a možnosti vytvárania prehľadov, sa môžu tiež značne líšiť.

Pri využívaní týchto nástrojov dochádza k nezrovnalostiam pri obnove a vykazovaní údajov nachádzajúcich sa v zariadení, ako napríklad neschopnosť obnoviť rezidentné údaje, nezrovnalosti medzi údajmi zobrazenými na pracovnej stanici a údajmi vygenerovanými vo výstupných správach, skrátené údaje vo vykazovanom alebo zobrazenom výstupe, chyby pri dekódovaní a preklade obnovených údajov a neschopnosť obnoviť všetky relevantné údaje. Príležitostne dochádza k tomu, že aktualizácie alebo nové verzie nástrojov sú v niektorých aspektoch menej schopné ako predchádzajúca verzia.

Nástroje by sa mali overiť, aby sa zabezpečila ich prijateľnosť a mali by sa znova použiť, keď budú k dispozícii aktualizácie alebo nové verzie nástroja. Tieto výsledky zohrávajú dôležitý faktor pri rozhodovaní o vhodnosti nástroja, ako kompenzovať prípadné nedostatky a či zvážiť použitie inej verzie alebo aktualizácie nástroja. Súčasné nástroje len zriedka poskytujú prostriedky na získanie podrobných protokolov extrakcie údajov. Vyšetrovateľ môže porovnať výstup niekoľkých nástrojov na overenie konzistentnosti výsledkov. Aj keď je overenie nástroja časovo náročné, je nevyhnutné ho dodržiavať. Ako meradlo kvality by forenzní špecialisti mali dostať aj primerané aktuálne školenie o nástrojoch a postupoch, ktoré používajú.

Dôležitou charakteristikou forenzného nástroja je jeho schopnosť zachovať integritu pôvodného zdroja údajov, ktorý sa získava, a tiež integritu extrahovaných údajov. Prvé sa

vykonáva zablokovaním alebo iným odstránením požiadaviek na zápis do zariadenia obsahujúceho údaje. Druhé uvedené sa vykonáva výpočtom kryptografického hašu obsahu vytvorených súborov dôkazov a opakovaným overovaním, či táto hodnota zostáva nezmenená počas životnosti týchto súborov. Zachovanie integrity nielenže zachováva dôveryhodnosť z právneho hľadiska, ale umožňuje aj následnému vyšetrovaniu použiť rovnaký základ na replikáciu analýzy.

4 BUDÚCNOSŤ DIGITÁLNYCH STÔP ULOŽENÝCH NA MOBILNÝCH ZARIADENIACH

Digitálna forenzná oblasť je reaktívna oblasť, a preto budúce trendy v analýze mobilných telefónov do značnej miery závisia od trendov v odvetví mobilných telefónov. Telefóny sa stávajú oveľa schopnejšími a zatiaľ čo zostáva trh pre telefóny len so základnou funkcionalitou, telefóny s vyššou funkčnosťou sú rozširujúcim sa trhom. Pojem inteligentný telefón prestáva byť aktuálny, keďže sa stáva štandardom. Pre forenzných vyšetrovateľov a analytikov je to pozitívne z dvoch dôvodov: telefóny budú mať väčšiu kapacitu, a teda budú obsahovať viac potenciálnych dôkazov, a priemysel sa stabilizuje na menší počet platforiem základných operačných systémov.

Šírenie špičkových inteligentných telefónov v spotrebiteľskom aj komerčnom sektore bude mať v konečnom dôsledku vplyv na forenzné vyšetrovanie. Zvýšená kapacita telefónov bude vyžadovať väčšiu analýzu na základe jednotlivých zariadení, ale môže poskytnúť lepší prehľad. Mobilné telefóny sú dátovým úložiskom, ktoré je do značnej miery oddelené od jednotlivých používateľov a je menej pravdepodobné, že budú pozmenené alebo sfalšované.

Počet operačných systémov mobilných telefónov a zariadení sa konsoliduje do samostatnej skupiny, do značnej miery nezávislej od hardvéru. To pomôže extrakcii údajov a analýze v skrátených krivkách učenia pre rôzne zariadenia, ako aj lepšiemu pochopeniu toho, čo je možné extrahovať pre každú platformu. Potreba spätného inžinierstva idiosynkrázií nájdených vo vlastných operačných systémoch alebo individuálnych implementáciách sa časom zníži.

Budúcnosť forenznej analýzy mobilných telefónov a zariadení bude vo väčšej miere zahŕňať reverzné inžinierstvo aplikácií tretích strán. Takéto aplikácie závisia od platformy, sú napísané buď pomocou natívnych súprav SDK alebo prostredníctvom sád nástrojov tretích strán a majú rôzny prístup k základnému operačnému systému. Pochopenie schopnosti a zámeru aplikácií tretích strán môže byť za určitých okolností životne dôležité pre forenzných analytikov, pretože môžu byť svojou povahou škodlivé, nepriamo napomáhať zločinu, poskytovať komunikačné mechanizmy mimo štandardných telefónnych systémov alebo uchovávať údaje forenznej hodnoty (buď lokálne alebo na externe hosťovaných serveroch). Aplikácie tretích strán sú tiež pravdepodobne bránami ku cloudovým službám, ktoré čoraz viac využívajú mobilné zariadenia. Forenzné dôsledky cloud computingu presahujú rámec tejto práce, ale musíte si byť vedomí ich existencie a myšlienky, že dôkazy existujú aj mimo samotného zariadenia.

Telefóny nižšej kategórie so základnou funkcionalitou budú naďalej existovať vo významných počtoch. Z digitálneho forenzného hľadiska sú tieto telefóny lacné a jednorazové a je ťažké prisúdiť vlastníctvo. Takáto analýza si vyžaduje väčšiu škálovateľnosť analýzy v situáciách, keď jednotlivec môže ovládať viacero telefónov, viacero skupín ovláda jeden telefón a pri rozsiahlych analýzach sociálnych sietí.

Súčasné prepojenia medzi pracovnými stanicami a notebookmi a telefónmi takmer výlučne vnímajú telefón ako satelitné zariadenie. Zlepšená konektivita medzi telefónmi a inými zdrojmi údajov to môže zmeniť a poskytnúť lepšie prepojenia medzi pripojenými systémami.

Zďaleka najzreteľnejším trendom je, že mobilné zariadenia budú aj naďalej dôležité vo forenznej analýze a budú zohrávať veľkú úlohu v občianskych aj trestných vyšetrovaniach.

ZÁVER

Zahraničná odborná literatúra v tejto oblasti jasne uvádza, do akej miery závisia získané informácie od získanej techniky, typu mobilného OS a podporných prvkov kriminalistického skúmania. Všetky vyššie zmienené a realizované výskumy naznačujú, že architektúra súborových systémov vyžaduje realizáciu konkrétnych techník, ktoré predstavujú problémy pri kriminalistickom skúmaní MZ. Výsledkom je taktiež skutočnosť, že overovanie extrahovaných informácii nie je triviálna úloha. Preto je dôležité dôkladné pochopenie zaistenej techniky (MZ), architektúry súborových systémov, funkcii kriminalistického skúmania a ich nástrojov, taxonómie informácii a aktivít používateľa, ktoré je možné vyhodnotiť ako kybernetickú bezpečnostnú hrozbu za účelom šírenia extrémizmu, a je ich teda potrebné považovať za kľúčové body, ktoré je nevyhnutné uznať a zapojiť aj do vyšetrovacích postupov v praxi. Pochopenie týchto kľúčových bodov podľa môjho názoru prispeje v značnej miere k vyšetrovaniu extrémistických udalostí a s tým súvisiacich trestných činov extrémizmu.

Keďže mobilné zariadenia sú populárnymi platformami pre rôzne aplikácie, môžu poskytnúť nevyhnutné dôkazy pri forenzných vyšetrovaniach. Tieto zariadenia často slúžia ako zdroj digitálnych dôkazov pri trestných činoch a obsahujú osobné informácie o jednotlivcovi, ako sú fotografie, heslá a ďalšie užitočné údaje. Mobilné zariadenia tiež ukazujú, kde sa jednotlivci v konkrétnom čase nachádzajú a s kým komunikovali. Informácie obsiahnuté v mobilných zariadeniach môžu byť nápomocné aj pri vyšetrovaní trestného činu, keď sú použité na krádež duševného vlastníctva.

Mobilné zariadenia môžu byť nástrojom trestného činu aj v prípade, ak sa používajú na odpočúvanie prevádzky bezdrôtovej siete. V posledných rokoch sa stalo rutinou, že vyšetrovatelia zaisťujú mobilné zariadenia ako dôkazy. Tieto zariadenia sú náročným zdrojom dôkazov, pretože údaje v nich sú nestále a na spracovanie rôznych zariadení sú potrebné rôzne nástroje. V súčasnosti sú nástroje a školenia v tejto oblasti obmedzené, ale vzhľadom na rýchly nárast ich používania sa pravdepodobne stanu jednou z oblastí s najväčším rastom v oblasti skúmania digitálnych dôkazov.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

AB RAHMAN N., CHOO K. 2015. Integrating digital forensic practices in cloud incident handling: A conceptual cloud incident handling model. In: KO R, CHOO K-KR (eds) Cloud Security Ecosystem. Syngress, an Imprint of Elsevier, Waltham, pp. 383–400, ISBN 978-0128015957.

ANGLANO C. 2014. Forensic analysis of WhatsApp messenger on android smartphones. Digit Investig 11(3):201–213 [online]. Dostupné na internete: Forensic Analysis of WhatsApp Messenger on Android Smartphones - arXiv (readkong.com)

ARIFFIN A., D'OORAZIO C., CHOO K-KR., SLAY J. 2013. iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner? In: Proceedings of the 8th International Conference on Availability, Reliability and Security, Regensburg, Germany, Sept 2–6, 2013 (IEEE), 375–382, ISBN 9781479910977.

AZFAR A., CHOO K-KR., LIU L. 2015. Forensic Taxonomy of Popular Android mHealth Apps. In: Proceedings of the 21st Americas Conference on Information Systems

CHUNG H., PARK J., LEE S., KANG C. 2012. Digital forensic investigation of cloud storage services. Digit Investig 9(2):81–95, ISSN 1742-2876.

GLISSON WB., STORER T., BUCHANAN-WOLLASTON J. 2013. An empirical comparison of data recovered from mobile forensic toolkits. Digit Investig 10(1):44–55, ISSN 1742-2876.

GRISPOS G., GLISSON WB., STORER T. 2015. Recovering residual forensic data from smartphone interactions with cloud storage providers. In: KO R, CHOO K-KR (eds) Cloud Security Ecosystem. Syngress, an Imprint of Elsevier, Waltham, , pp. 383–400, ISBN 978-0128015957.

LEOM MD., DORAZIO CJ., DEEGAN G., CHOO K-KR. 2015. Forensic Collection and Analysis of Thumbnails in Android. In: Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communication, Helsinki, Finland, Aug 20–22, (IEEE) 1059–1066 ISBN 978-1-6654-1658-0.

MARTINI B., DO Q., CHOO K-KR. 2015. Mobile cloud forensics: An analysis of seven popular Android apps. In: KO R, CHOO K-KR (eds) Cloud Security Ecosystem. Syngress, an Imprint of Elsevier, Waltham, pp. 309–345, ISBN 978-0128015957.

MCMILLAN JER., GLISSON WB., BROMBY M. 2013. Investigating the increase in mobile phone evidence in criminal activities. In: Hawaii International Conference on System Sciences, Wailea, Hawaii, Jan 7–10, 2013 (IEEE), 4900–4909 a Berman KJ, Glisson WB, Glisson LM (2015) Investigating the Impact of Global Positioning System Evidence. In: Hawaii International Conference on System Sciences, Hawaii, Jan 5–8, 2015 (IEEE), 5234–5243

PORADA, V., STRAUS, J. 2012. Kriminalistické stopy, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2012 s. 302, ISBN 978-80-7380-396-4

PORADA V. 2019. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. Plzeň:Aleš Čenek, s.180, ISBN 978-80-7380-741-2

SGARAS C., KECHADI M-T., LE-KHAC N-A. 2015. Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications. In: Garain U, Shafait F (eds) Computational Forensics. Springer, Switzerland, pp. 188–199, ISBN 978-3-319-20124-5.

TASSONE C., MARTINI B., CHOO K-KR., SLAY J. 2013. Mobile device forensics: a snapshot. Trends issues crime Crim. Justice no. 460: 1– 7. Australian Institute of Criminology, Canberra, ISSN 1836-2206.

npor. JUDr. Milan KUSÁK
Borovianska cesta 1, 060 01 Zvolen
milan.kusak@akademiapz.sk

LEGITIMITA OBMEDZENÍ PODNIKANIA PROFESIONÁLNYCH VOJAKOV

LEGITIMACY OF RESTRICTIONS ON BUSINESS OF PROFESSIONAL SOLDIERS

Tomáš MARTAUS, Sarah ŠAJBANOVÁ

ABSTRACT

The presented contribution provides an insight into the legal regulation of restrictions on one of the basic rights and freedoms guaranteed by the Constitution of the Slovak Republic, such as the right to do business. As part of its analytical part, it reflects on its constitutionality as well as a comparison with similar legislation of the Czech Republic. In the core of the paper, you can also find the conclusions of a survey conducted using the questionnaire method, focused on the interest in the implementation of this constitutional right by professional soldiers of the Slovak Republic. As well as the public's view of its application in the armed forces.

Keywords: professional soldier, business, constitution

ÚVOD

Vďaka svojmu vrcholnému postaveniu v hierarchii právnych predpisov upravuje Ústava Slovenskej republiky už tretie desaťročie tie najdôležitejšie spoločenské vzťahy. Medzi takéto vzťahy rozhodne patrí i garancia základných práv a slobôd.

Ich základný charakter deklaruje Ústava Slovenskej republiky v čl. 12 ods. 2, keď konštatuje, že „základné práva a slobody sa zaručujú na území Slovenskej republiky všetkým bez ohľadu na pohlavie, rasu, farbu pleti, jazyk, vieru a náboženstvo, politické, či iné zmýšľanie, národný alebo sociálny pôvod, príslušnosť k národnosti alebo etnickej skupine, majetok, rod alebo iné postavenie. Nikoho nemožno z týchto dôvodov poškodzovať, zvýhodňovať alebo znevýhodňovať.“ (Ústava Slovenskej republiky, čl. 12 ods. 2)

Existenciu takéhoto charakteru základných práv a slobôd v našom právnom poriadku súčasne potvrdzuje i Listina základných práv a slobôd, v zmysle ktorej „základné práva a slobody sa zaručujú všetkým bez rozdielu pohlavia, rasy, farby pleti, jazyka, viery a náboženstva, politického či iného zmýšľania, národného alebo sociálneho pôvodu, príslušnosti k národnostnej alebo etnickej menšine, majetku, rodu alebo iného postavenia.“ (Listina základných práv a slobôd, čl. 3 ods. 1)

Predmetné východisko tak zabezpečuje bezpodmienečnú rovnosť ľudí v ich základných právach a slobodách.

1 PROFESIONÁLNI VOJACI OZBROJENÝCH SÍL SLOVENSKEJ REPUBLIKY A PRÁVO NA PODNIKANIE

S výnimkou zákazu mučenia či neľudského a ponižujúceho zaobchádzania vyjadreného v čl. 16 ods. 2 Ústavy Slovenskej republiky umožňuje právny systém v oprávnených prípadoch zásah do ľudských práv a slobôd v podobe ich obmedzenia.

Inak tomu nie je ani v prípade profesionálnych vojakov Ozbrojených síl Slovenskej republiky. Povaha poslania ich profesie totiž v zásade pripúšťa obmedzenie tých práv a slobôd, ktorých neobmedzené uplatňovanie je schopné ohroziť riadne plnenie ich povinností. V zmysle § 4 zákona č. 321/2002 Z.z. o ozbrojených silách Slovenskej republiky je hlavnou úlohou ozbrojených síl „brániť Slovenskú republiku pred napadnutím cudzou mocou, brániť jej zvrchovanosť, územnú celistvosť, nedotknuteľnosť hraníc a plniť záväzky vyplývajúce z medzinárodných zmlúv, ktorými je Slovenská republika viazaná“ (Zákon o ozbrojených silách Slovenskej republiky, § 4 ods. 1)

Podľa čl. 35 ods. 1 Ústavy Slovenskej republiky má každý právo podnikať či uskutočňovať inú zárobkovú činnosť. Ide pritom o špeciálne ústavné právo vo vzťahu ku právu slobodne sa rozhodnúť vykonávať určité zvolené povolanie, takisto garantované čl. 35 ústavy. (Ústavné garancie ľudských práv, 2004)

Čl. 54 ústavy však umožňuje právo podnikať či vykonávať inú hospodársku činnosť obmedziť v prípade špecifických štátnych orgánov, pri ktorých by v prípade plnenia ich ústavných práv mohlo dôjsť k znefunkčneniu činnosti štátnych orgánov. (Komentár k Ústave Slovenskej republiky, 1997) Ústava medzi takéto orgány radí aj Ozbrojené sily Slovenskej republiky, resp. ich príslušníkov a tak deleguje prijatie zákona, ktorý je oprávnený uvedené práva obmedziť.

Pokiaľ sa analyticky pozrieme na zákon o štátnej službe profesionálnych vojakov v platnom znení, zistíme, že profesionálnemu vojakovi zakazuje podnikať, vykonávať inú zárobkovú činnosť či členstvo v riadiacich, kontrolných alebo dozorných orgánoch právnických osôb vykonávajúcich podnikateľskú činnosť. (Zákon o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov, § 13 ods. 1)

I napriek uvedenému zákazu však zákon pripúšťa taxatívny okruh činností, ktoré profesionálny vojak môže za odplatu vykonávať, avšak nie formou podnikania, kde v zmysle § 13 zákona o štátnej službe profesionálnych vojakov panuje bezvýnimočný zákaz. Ide tak napríklad o pedagogickú, trénerskú, tlmočnícku činnosť, či lekársku, veterinárnu činnosť alebo činnosť vedúceho tábora pre deti a mládež.

Je však otázne, či takýto rozsah výnimiek z obmedzenia základného práva na podnikanie a výkon inej zárobkovej činnosti je z ústavného hľadiska postačujúci. Z taxatívne stanovených výnimiek vyplýva, že ide o výnimky, pri ktorých možno nájsť verejný či spoločensky prospešný záujem na ich výkone. No výkon týchto činností vie de facto profesionálneho vojaka obmedziť v rovnakom, ak nie aj vo väčšom rozsahu, ako podnikateľská činnosť fitness-trénera, výživového poradcu, lektora, či drobného obchodníka s militáriami a pod. Nejde teda o výnimky, ktoré by samé o sebe nemali vplyv na plnenie povinností profesionálneho vojaka.

Sme preto názoru, že vzhľadom na uvedené je potrebné vecne sa zamýšľať nad vymedzením kritérií stanovenia činností, ktoré profesionálnemu vojakovi môžu brániť v plnení jeho povinností v závislosti na ich špecifickom charaktere. Môže tak ísť o výkon nebezpečných činností ohrozujúcich jeho zdravotnú spôsobilosť alebo vplývajúcich na možnosť jeho radikalizácie a pod.

Uvedené podporuje i komparácia s českým právnym poriadkom, nakoľko zákon o vojácích z povolání č. 221/1999 Sb. v § 19 ods. 1 písm. j) umožňuje vojakovi z povolania Armády Českej republiky so súhlasom služobného orgánu vykonávať zárobkovú činnosť.

Na základe § 47 tohto zákona, môže vojak v zmysle udeleného súhlasu vykonávať zárobkovú činnosť, ktorá neovplyvní výkon jeho služby alebo iný dôležitý záujem služby. Taxatívny zákaz v prípade jeho činnosti zákon stanovuje výlučne pre činnosť zodpovedného zástupcu podľa osobitných predpisov, člena štatutárneho alebo kontrolného orgánu právnickej osoby, ktorá realizuje podnikateľskú činnosť, s výnimkou členstva v štatutárnych alebo kontrolných orgánoch nestavebných bytových družstiev zriadených ku správe bytového

fondu, a právnických osôb a organizačných zložiek štátu, ktorých zriaďovateľom alebo zakladateľom je ministerstvo obrany alebo iný správny úrad. (Zákon o vojácích z povolání, § 47)

2 PROFESIONÁLNI VOJACI A ICH ZÁUJEM O PODNIKANIE

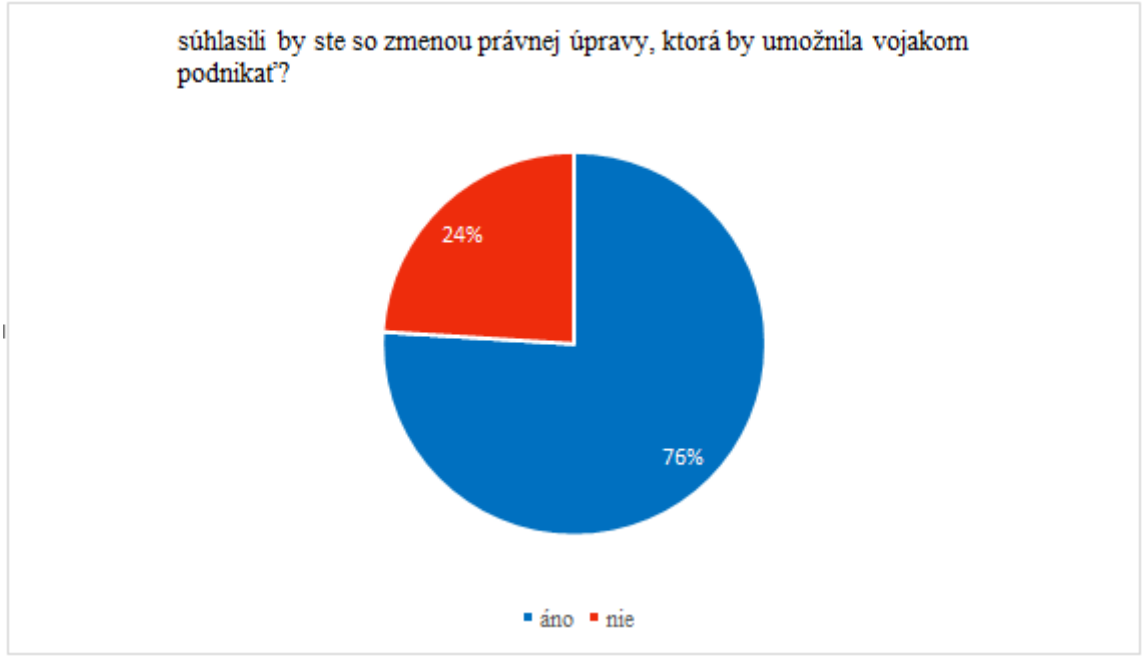
S ohľadom na českú právnu úpravu, ktorá s veľmi špecifickým a útlym obmedzením umožňuje na základe udeleného súhlasu profesionálnym vojakom vykonávať zárobkovú činnosť, sme dotazníkovou metódou skúmali na vybranej vzorke profesionálnych vojakov ich záujem o zmenu právnej úpravy po vzore tej českej.

V priebehu mesiaca august 2022 sme s dotazníkovými otázkami oslovili 25 civilných osôb mimo Ozbrojených síl Slovenskej republiky, 39 profesionálnych vojakov a 19 profesionálnych vojakov vykonávajúcich veliteľskú funkciu. V rámci neho nás zaujímali odpovede respondentov na otázky či by súhlasili so zmenou právnej úpravy, ktorá by profesionálnym vojakom umožnila podnikať. V prípade profesionálnych vojakov nás zaujímala skutočnosť či by takúto možnosť podnikať aj využili a pokiaľ áno, v akej oblasti by radi vykonávali svoju podnikateľskú činnosť. Všetky zaslané dotazníky boli vyplnené úplne, a tak pre náš prieskum kompletne využiteľné.

Z vyhodnotenia zozbieraných dát plynie, že tri štvrtiny opýtaných civilných osôb by súhlasilo so zmenou zákonnej úpravy, ktorá by profesionálnym vojakom umožnila realizovať vlastnú podnikateľskú činnosť (graf č.1). Túto možnosť by uvítala drvivá väčšina profesionálnych vojakov (82% - graf č. 2) ako aj väčšina (58% - graf č. 3) ich veliteľov.

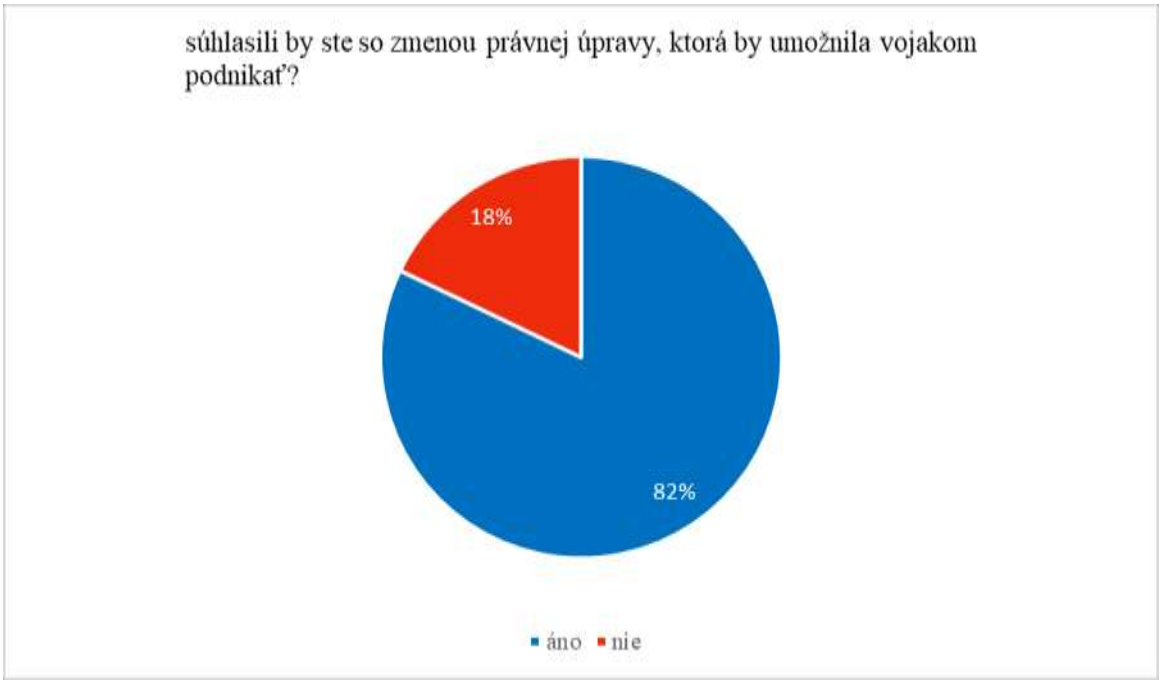
Možnosť podnikať by reálne využilo takmer 80% opýtaných profesionálnych vojakov (graf č. 4) a každý druhý ich veliteľ (graf č. 5).

Svoje aktivity by pritom najčastejšie realizovali v oblasti gastronómie, obchodu s nehnuteľnosťami, prevádzkovania strelnice, obchodovania s militáriami, v oblasti informačných technológií a stavebníctva.



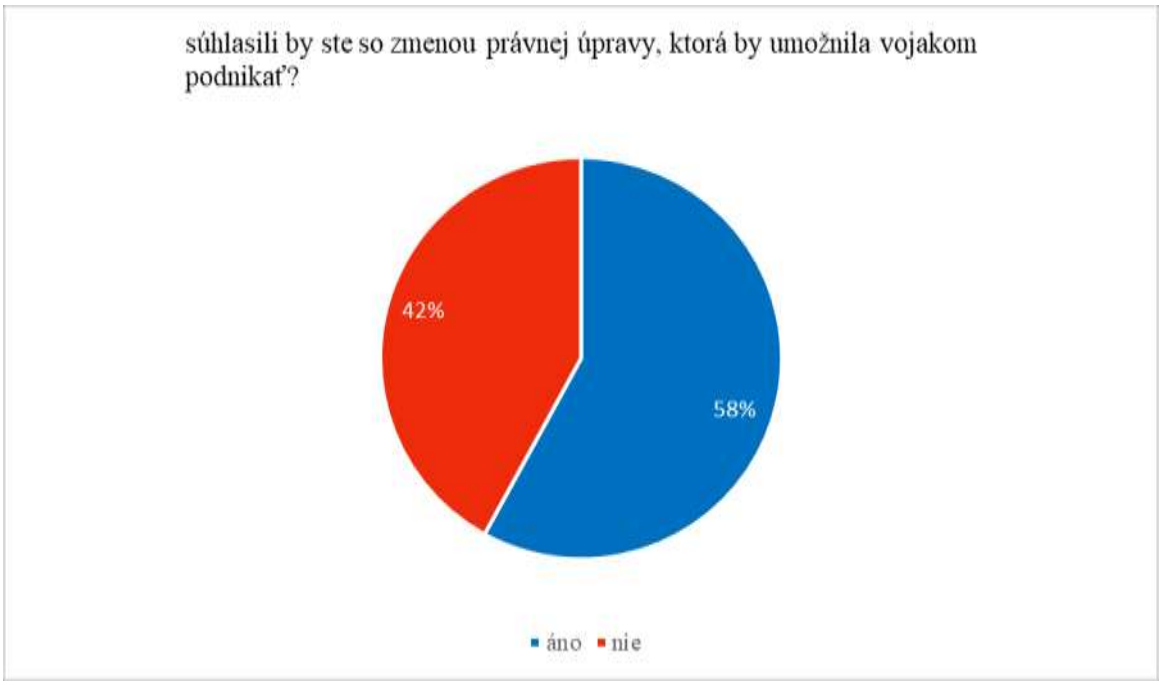
Graf č. 1 Odpovede civilnej verejnosti na otázku či by umožnila vojakom podnikať

Zdroj: vlastné spracovanie



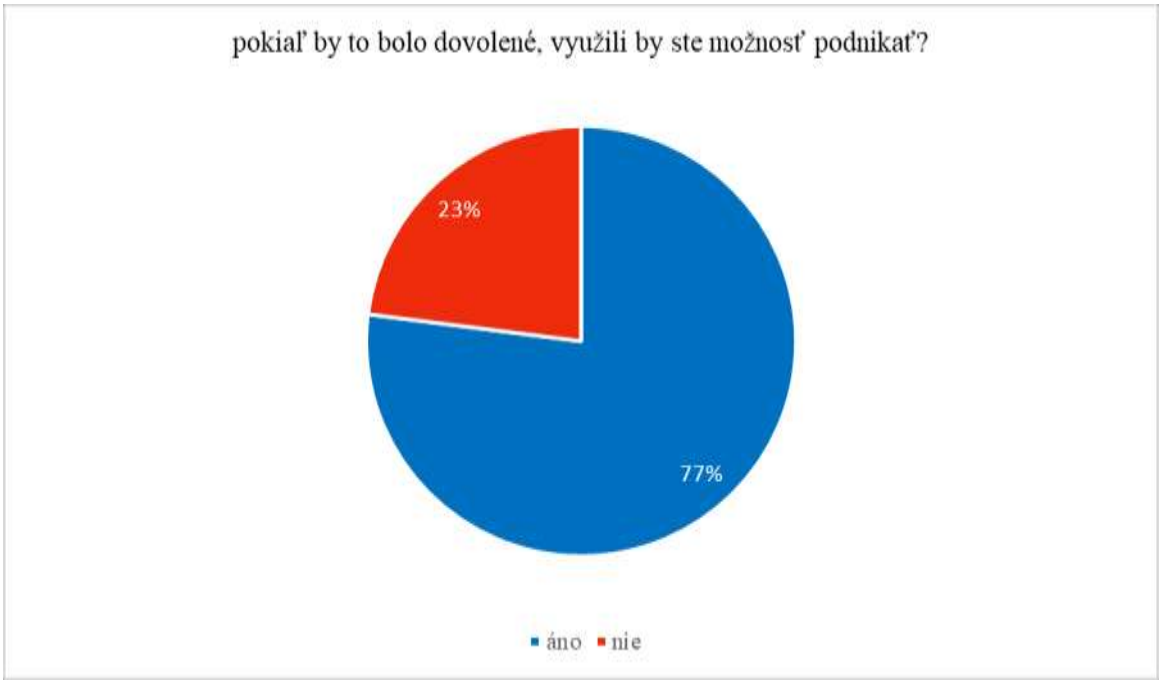
Graf č. 2 Odpovede profesionálnych vojakov na otázku či by súhlasili so zmenou zákona, ktorá im umožní podnikať

Zdroj: vlastné spracovanie



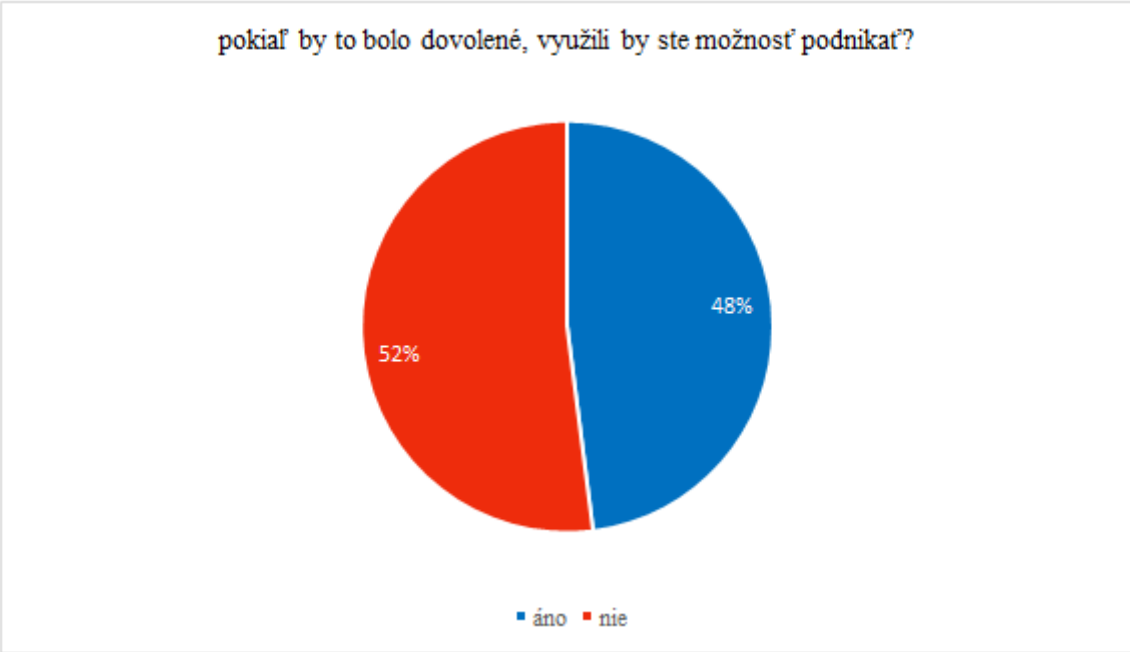
Graf č. 3 Odpovede veliteľov na otázku či by súhlasili so zmenou zákona, ktorá im umožní podnikať

Zdroj: vlastné spracovanie



Graf č. 4 Odpovede profesionálnych vojakov na otázku či by využili možnosť podnikať

Zdroj: vlastné spracovanie



Graf č. 5 Odpovede veliteľov na otázku či by využili možnosť podnikať

Zdroj: vlastné spracovanie

3 Z ROZHODOVACEJ ČINNOSTI ÚSTAVNÉHO SÚDU SLOVENSKEJ REPUBLIKY

Zaujímavým je i pohľad na zákonné obmedzenia práva podnikať, vykonávať zárobkovú činnosť v prípade štátnej služby profesionálneho vojaka v kontexte záverov judikatúry Ústavného súdu Slovenskej republiky.

Základné východisko nazerania Ústavného súdu Slovenskej republiky na slobodu podnikania tkvie v charaktere druhej generácie ľudských práv, medzi ktoré sa radí i právo na podnikanie. „Právo podnikať je zahrnuté do piateho oddielu druhej hlavy ústavy. Tým sa predurčujú základné vlastnosti tohto práva, aj podmienky jeho uplatňovania, lebo základné práva a slobody prvej generácie sa zaručujú v ústavnom režime, aký nie je totožný s ústavnou ochranou základných práv a slobôd náležiacich do druhej generácie základných práv a slobôd. Základné práva z piateho oddielu druhej hlavy ústavy sú právami z druhej generácie ľudských práv. Ide o základné práva usporiadané na tri podskupiny – hospodárske, sociálne a kultúrne – zavedené oficiálne, medzinárodnými dohovormi o ľudských právach, ktoré ich priznali. ... Základné práva a slobody prvej generácie sú oprávneným osobám dostupné iným spôsobom a za iných podmienok ako základné práva a slobody druhej generácie.“ (PL ÚS 14/2014)

V prípade druhej generácie ľudských práv tak ide o skupinu oprávnení, ktorých sa možno domáhať výlučne v medziach zákonov, ktoré tieto ustanovenia vykonávajú, čím „ústava poskytuje zákonodarcovi nepochybne väčší priestor (v porovnaní s inými skupinami základných práv a slobôd) pre voľnú úvahu (uváženie) na účely určenia, v akom rozsahu, kvalite a za akých podmienok bude garantovať hospodárske, sociálne a kultúrne práva a slobody.“ (PL. ÚS 11/2013)

Podstatnou však je skutočnosť, že v prípade priestoru pre uváženie prenechané zákonodarcovi „ústavný súd už vyslovil právny názor, že priestor pre voľnú úvahu poskytnutý ústavou zákonodarcovi pri prijímaní týchto zákonov nemožno chápať absolútne; jej limity treba hľadať predovšetkým v ústavných princípoch a v požiadavke ochrany ďalších hodnôt, na ktorých je ústava založená a ktoré chráni. Tieto základné práva už svojou povahou síce nabádajú na právnu úpravu zo strany štátu (ktorá naplní jeho obsah), ten však nesmie zasiahnuť samotnú podstatu týchto práv ani sa dotknúť iných práv zakotvených v ústave a Dohovore o ochrane ľudských práv a základných slobôd.“ (PL. ÚS 8/2014)

Podobne tak i z Nálezu Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 14/2018 z 10. novembra 2021 plynie, že v spojení so zákonnými zásahmi do ústavou garantovaného práva podnikať možno pripustiť výlučne zúženie možnosti realizácie základného práva podnikať, a to tak aby tento zásah nezasahoval do „zmyslu a rozsahu, resp. obsahu tohto základného práva“ (PL. ÚS 14/2018). Z predmetného rozhodnutia pléna ústavného súdu tak vyplýva, že právo na podnikanie nemožno odoprieť úplne.

Uvedenému korešponduje i znenie čl. 54 Ústavy Slovenskej republiky, ktoré hovorí výlučne o „obmedzení“ tohto práva, ako aj čl. 12 ods. 1, v zmysle ktorého sú základné práva a slobody „nezrušiteľné“ či „neodňateľné“.

Práve uvedené sa však dostáva do priameho konfliktu so znením § 13 ods. 1 písm. a) zákona o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov, v zmysle ktorého profesionálny vojak podnikať nesmie.

ZÁVER

Na základe analytickej časti predkladaného príspevku, zaoberajúcej sa platným a účinným znením základného právneho predpisu upravujúceho spoločenské vzťahy v oblasti výkonu štátnej služby profesionálneho vojaka a jeho komparácii s ústavne prípustnými limitmi stanovenými ako Ústavou slovenskej republiky, tak i rozhodovacou činnosťou pléna

Ústavného súdu Slovenskej republiky, si záverom príspevku dovolíme vysloviť svoj názor o pochybnostiach ohľadom ústavnosti odňatia práva podnikať v prípadoch výkonu štátnej služby profesionálnym vojakom.

Vzhľadom na toto presvedčenie, ako i s ohľadom na komparáciu s právnym poriadkom Českej republiky, či vzhľadom na prejavený záujem podnikať vo vybranej vzorke príslušníkov Ozbrojených síl Slovenskej republiky, tak považujeme za vhodné zmeniť platné znenie zákona o štátnej službe profesionálnych vojakov. A to tak, aby profesionálnym vojakom umožňovalo vo výnimočných prípadoch, priamo neobmedzujúcich plnenie úloh Ozbrojených síl Slovenskej republiky, realizovať svoje právo na podnikanie.

Nakoľko profesionálny vojak je v závislosti od svojej funkcie a svojej odbornosti potrebný pre Ozbrojené sily Slovenskej republiky v rozličnej špecifickej miere, ako vhodný vnímame český model právnej úpravy, ktorá umožňuje takéto situácie posudzovať ad hoc v závislosti od zohľadnenia všetkých jedinečností posudzovaného prípadu.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ČIČ, M. a kol.: Komentár k Ústave Slovenskej republiky. Martin: vydavateľstvo Matice slovenskej, 1997

KRÁĽ, J. a kol.: Učebné texty právnickej fakulty. Bratislava: GUPRESS, 2004

Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 8/2014 zo 27. mája 2015

Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 11/2013 zo 22. októbra 2014

Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 14/2014 zo 4. novembra 2015

Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 14/2018 z 10. novembra 2011

Obmedzenia niektorých ústavných práv profesionálnych vojakov [online], Comenius, [7. sept. 2017], dostupné na: https://comeniuscasopis.flaw.uniba.sk/2017/09/07/obmedzenia-niektorych-ustavnych-prav-profesionalnych-vojakov/

Ústava Slovenskej republiky č. 460/1992 Zb.

Zákon o ozbrojených silách Slovenskej republiky č. 321/2002 Z. z.

Zákon o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov č. 281/2015 Z.z.

Zákon o vojácích z povolání, č. 221/1999 Sb.

JUDr. Tomáš MARTAUS
Akadémia ozbrojených síl gen. M. R. Štefánika
tomas.martaus@aos.sk

Sarah ŠAJBANOVÁ
Akadémia ozbrojených síl gen. M. R. Štefánika
sarah.sajbanova@aos.sk

ANALÝZA STRATÉGIE VNÚTORNEJ BEZPEČNOSTI EÚ - SMEROM K EURÓPSKEMU BEZPEČNOSTNÉMU MODELU

ANALYSIS OF THE EU INTERNAL SECURITY STRATEGY - TOWARDS A EUROPEAN SECURITY MODEL

Miroslav MUŠINKA

ABSTRACT

People living in one region desire to live in safety, which is one of the basic needs of man. That's why they've been forming different communities, coalitions, unions since time immemorial. This is not the case in the region of Europe only. This work deals with the establischment and development of internal security in Europe and, following the creation of the European Union, also in the European Union. It aims to analyse the establishment and development of the Union's internal security and to clarify the focus of the EU Internal Security Strategy as a fundamental policy for ensuring the security of EU citizens. The first part deals with the definition of the European Union's security area. The second part described the historical development of security in Europe. The third part deals with the internal security of the Union. The fourth part describes the most serious threats affecting the internal security of the Union.

Keywords: Safety, Europe, European Union, contract, plan, cooperation, security, strategy.

ÚVOD

Už od vzniku prvotnej myšlienky na jednotnú Európu bola jej motívom ekonomická prosperita, spolupráca a zachovanie bezpečnosti. Prvým počinom smerom k jednotnej Európe bol vznik Európskeho spoločenstva pre uhlie a oceľ v roku 1951. Jeho hlavným cieľom bolo vytvoriť spoločný medzinárodný trh s uhlím, koksom, oceľou, železnou rudou a šrotom, a takouto hospodárskou spoluprácou zabrániť vypuknutiu ďalšej vojny v Európe (Zmluva o ESUO, 1951).

Neskôr, po samotnom vzniku Európskej Únie (EÚ), bola potreba zabezpečovania bezpečnosti EÚ zakotvená aj v právnom akte - zakladajúcej zmluve, tzv. Maastrichtskej zmluve o Európskej únii. Zmluva (EUR-Lex, 2012), okrem iného, definovala tri základné piliere EÚ:

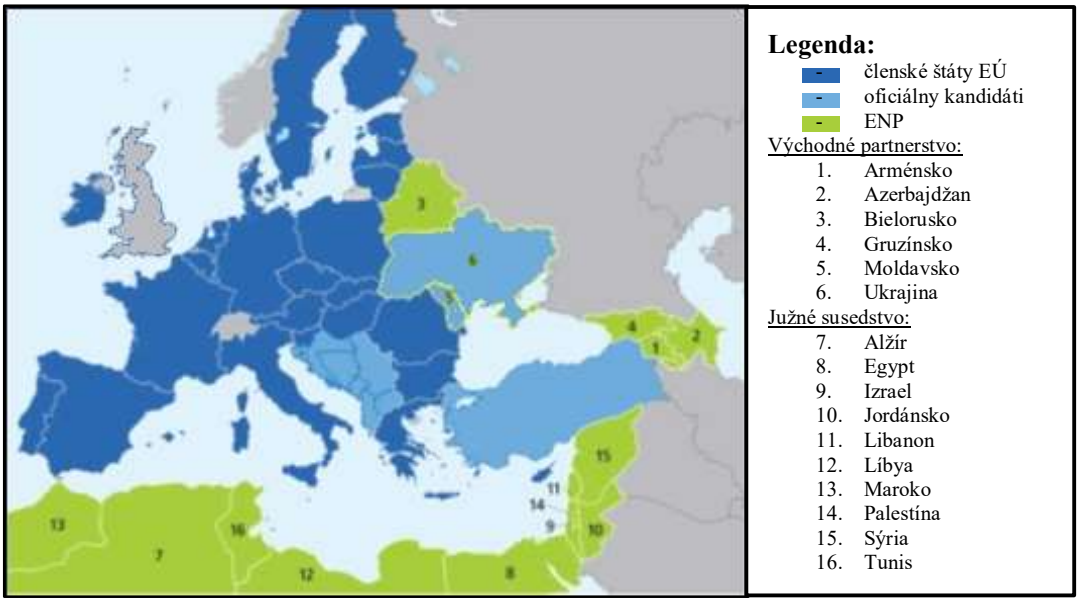
- 1. pilier - európske spoločenstvá,
- 2. pilier – spoločná zahraničná a bezpečnostná politika,
- 3. pilier – spolupráca v oblasti spravodlivosti a vnútorných vecí.

Práve 2. pilier mal za cieľ zabezpečiť pre občanov EÚ maximálnu úroveň bezpečnosti. Zakladajúce štáty a štáty pri vstupe do EÚ sa zaviazali dodržiavať ľudské práva, zásady právneho štátu a solidarity. To znamená, že bezpečnosť je pre obyvateľov EÚ jednou z hlavných priorít (Európska únia, 2010). Spoločná a jednotná EÚ a s ňou spojené odstránenie kontrol na vnútorných hraniciach jednotlivých štátov (tzv. Schengenský priestor) dáva občanom EÚ možnosť slobodne cestovať, študovať, obchodovať či pracovať (Turaj, 2021).

Odstránenie hraničných kontrol a voľnosťou pohybu v celej EÚ umožňuje nie len vyššie spomínaný demokratické činnosti, ale umožňuje šírenie hrozieb, ktoré sa vytvárajú vo vnútri EÚ. Je pravda, že hrozby, ako je napr. počítačová kriminalita, nepoznajú geografické hranice.

Práve z tohto dôvodu sa zahraničná a bezpečnostná politika zameriava okrem iného aj na prevenciu proti hrozbám mimo hraníc EÚ. Dôraz kladie na podporu a stabilizovanie bezpečnosti najmä v susediacich krajinách. EÚ pre susedné štáty poskytuje pomoc prostredníctvom hospodárskeho rozvoja, zamestnanosti v rámci EÚ, programov zameraných na mládež, dopravu, energetickú prepojenosť, mobilitu, bezpečnosť a migráciu, odborné poradenstvo v oblasti verejnej správy, práva a ľudských práv prostredníctvom politiky pod názvom Európska Susedská Politika (European Neighbourhood Policy - ENP). ENP definuje vzťahy EÚ so 16 najbližšími východnými a južnými susednými štátmi EÚ (Obrázok 1). Týmto sa ENP, ako kľúčový prvok európskej zahraničnej politiky, zameriava na stabilizáciu regiónu v politickej, hospodárskej a bezpečnostnej oblasti (Furness-Schäfer, 2015).

Cieľom príspevku je analyzovať vznik a proces vzniku a inštitucionalizácie systému vnútornej bezpečnosti EÚ a objasniť zameranie Stratégie vnútornej bezpečnosti EÚ ako základnej politiky pre zabezpečovanie bezpečnosti občanov EÚ. Čiastkovou úlohou je definovať vnútorné bezpečnostné prostredie EÚ a priblížiť najväčšie hrozby bezpečnosti EÚ. Príspevku majú prehľadový charakter. Hlavným prínosom je časovo historické zosumarizovanie vzniku a vývoja vnútornej bezpečnosti EÚ od obdobia Vestfálskeho mieru po vznik Stratégie vnútornej bezpečnosti EÚ. Ďalším prínosom je teoretické vymedzenie vnútorného bezpečnostného prostredia EÚ pre jasné pochopenie vnútornej bezpečnosti EÚ a opísanie najzávažnejších hrozieb, ktoré vplývajú na toto prostredie.



Obrázok 1 Európska susedská politika.
Zdroj: https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/structure_sk#header_countries_list (upravené autorom)

1 VNÚTORNÉ BEZPEČNOSTNÉ PROSTREDIE EÚ

Každý človek sa vo svojom živote potrebuje cítiť bezpečne. Pre zabezpečenie tejto potreby musí EÚ každý deň zabezpečovať bezpečnosť svojich občanov (S&D, s. a.). „*Vnútorná bezpečnosť v Európe je otázkou práva človeka žiť bez strachu*“ (S&D, s. a., s. 3). Cieľom premysleného, cieľavedomého a komplexného pôsobenia výkonnej moci, ktorú predstavuje každá vláda štátu EÚ, je teda kvalitný a bezpečný život svojich občanov (Brezula, 2020).

V dnešnej dobe sa pojem bezpečnostné prostredie objavuje takmer vo všetkých strategických dokumentoch, študijných materiáloch a literatúre, ktorá sa venuje bezpečnosti, tak i v diskusiách a textoch z tejto oblasti. Analýza bezpečnostného prostredia má kľúčový význam pre prácu bezpečnostných analytikov, pretože iba na základe analýz bezpečnostného prostredia môžeme vyhodnocovať bezpečnostné hrozby, ktoré by mohli pôsobiť alebo pôsobia na objekt bezpečnosti (Porada a kol., 2019).

Bezpečnostné prostredie EU je možné definovať aj ako prostredie v ktorom objekt, presadzuje svoje bezpečnostné záujmy v interakcií s nositeľmi identifikovaných bezpečnostných hrozieb. Je nutné taktiež brať do úvahy fakt, že bezpečnostné prostredie EÚ, ktoré je tvorené samostatnými subjektami, nie je stabilný nemenný systém. Práve naopak, je to zložitý a dynamicky sa vyvíjajúci systém, ktorý sa stáva sa zložitejším, tak ako vstupujú nové faktory a vznikajú nové interakcie medzi subjektami v rámci bezpečnostného prostredia EÚ (Tvaruška, 2018).

Z pohľadu utvárania pocitu bezpečnosti v EÚ, čiže v určitom priestore, je možné hovoriť o bezpečnostnom prostredí. Charakterizovať bezpečnostné prostredie je pomerne zložitý a komplexný problém. Prístupy k hodnoteniu bezpečnostného prostredia sú často diametrálne odlišné, čo do metodiky tak do rozsahu a hĺbky. Východiskom je dôkladné zadefinovanie priestoru, ktorý má byť posudzovaný z bezpečnostného hľadiska. Snahou o poňatie bezpečnostného prostredia EÚ v jeho plnom rozsahu a obsahu by malo byť úsilie o celkový a komplexný pohľad. Bezpečnostné prostredie je každé prostredie, v ktorom sa realizujú bezpečnostné záujmy a uskutočňujú bezpečnostné vzťahy (Hofreiter, 2016).

Po analýze príspevkov o hodnotení bezpečnosti a hodnotení bezpečnostného prostredia od rôznych autorov v obore securitológie je možné zovšeobecniť, že časť prírodného, spoločenského a technogenného prostredia, v ktorom sú podmienky existencie a vývoja sociálneho prostredia subjektov, ich činnosti, vzťahy a záujmy zamerané na bezpečnosť je bezpečnostné prostredie. Takéto prostredie je charakterizované na určitom území, ktoré je relatívne sociálne ucelené, a spravidla je podmienené aj ďalšími sociálno-ekonomickými, demografickými, vojensko-strategickými a kultúrnohistorickými vzťahmi. Bezpečnostné prostredie nie je možné chápať iba ako priestor vymedzený hranicami (ako napr. mesto, okres, štát, kontinent), alebo iba ako vzťahy medzi určitými spoločenskými, politickými či dokonca vojenskými aktérmi.

Keďže cieľom tohto príspevku je analyzovanie vzniku a vývoja vnútornej bezpečnosti EÚ, preto na tento účel bude za bezpečnostné prostredie EÚ považované geografické územie členských štátov, ktorého hranicu tvoria hranice členských štátov EÚ susediace so štátmi, ktoré nie sú členmi EÚ. V podstate je možné vnútorné bezpečnostné prostredie EÚ chápať ako bezpečnostné prostredie jednotlivých členských štátov EÚ. Toto je ale iba tzv. geografický rámec vnímania bezpečnostného prostredia (Hofreiter, 2016).

Bezpečnostná situácia a problémy jednotlivých členských štátov sú natoľko previazané v rámci spoločenstva - únie, že problémy národnej bezpečnosti každého z nich nie je možné primeraným spôsobom analyzovať samostatne (Laml, 2014) preto budeme analyzovať výzvy vnútornej bezpečnosti, ktoré sú spoločné pre celú úniu. Z pohľadu takéhoto prístupu sa jedná o tzv. široký prístup Kodanskej školy k bezpečnosti, ktorý je komplexnejší a bezpečnostné prostredie v rámci určitého geografického územia skúma z vojenského, politického, ekonomického, environmentálneho a sociálneho pohľadu (Laml, 2014).

Ďalšou dimenziou skúmania bezpečnostného prostredia je tzv. priestorová dimenzia. Pod priestorovou dimenziou je nutné chápať pôsobenie jednotlivých prvkov bezpečnostného prostredia najmä vo vzťahu k hrozbám a priestorom. Konkrétne sa jedná o priestory pozemné, vodné, vzdušné, vesmírne, kybernetické a mikrosvet (Laml, 2014). Ako už bolo naznačené, v dnešnej dobe najväčšie hrozby pochádzajú najmä z kybernetického prostredia. Toto prostredie nepozná hranice medzi jednotlivými štátmi, je masovo prístupný, využívaný vo

veľkej miere jednotlivcom, skupinou ale aj veľkým spoločenstvom. Hrozby z kybernetického prostredia môžu mať ďalekosiahle následky aj pre veľké spoločenstvá. Často prichádzajú neočakávane, nie je jednoduché ich včas identifikovať a častokrát je náročné vystopovať ich pôvodcu a zistiť ich skutočný zámer. Práve z týchto dôvodov je tejto hrozbe v posledných rokoch venovaná veľká pozornosť a dostáva sa na popredné miesta v akčných plánoch pre prevenciu voči hrozbám.

2 HISTÓRIA A VÝVOJ SPOLOČNEJ BEZPEČNOSTI V EURÓPE

Myšlienka zjednotenej Európy sa opakovane objavovala v jej dejinách v rôznych podobách (Fiala, Pitrová, 2003). Dôvody pre zjednotenie sa však postupom času menili v závislosti najmä od politických a mocenských okolnosti. Častým dôvodom pre zjednotenie Európy bola mocenská snaha, čiže snaha ovládať čo najväčšie územie a profitovať z výhod nadvlády nad takýmto rozsiahlym územím. Jednou z nesporných výhod takéhoto mocenstva bola aj bezpečnosť. Snahou zjednotiť čo najviac krajín do jednej únie by sa eliminovali vojenské hrozby medzi jednotlivými krajinami, a naopak veľké a zjednotené spoločenstvo znamenalo väčšiu armádu, a tá mohla lepšie reagovať na vojenské hrozby spoza hraníc spoločenstva (Fiala, Pitrová, 2003).

2.1 PRVOPOČIATKY ZABEZPEČOVANIA MIERU V EURÓPE AKO CELKU

Jednu z prvých myšlienok na jednotné európske spoločenstvo rozvíjal už v 14 str. francúzsky právnik a politický reformátor P. Dubois. Dubois sa presadzovaním svojej myšlienky snažil o politickú a vojenskú jednotnosť v rámci európskych panovníckych rodov a tým vytvoriť odolnejšiu obranu hlavne pred hrozbami arabských nájazdov (Fiala, Pitrová, 2003).

V 15. – 16. storočí sa Európa vyznačovala v podstate jednotou, ktorá bola založená na báze kresťanského vierovyznania na celom svojom území. Táto jednota umožňovala organizovanejšie vedenie vojen na obranu proti arabským snahám podriadiť si Európu. V 17. storočí inteligencia, hlavne vo francúzsku ale aj v ostatných krajinách, začína presadzovať myšlienku práv a slobôd jednotlivca pred autokraciou zo strany vtedajších panovníkov a vladárov. To prerástlo do konfliktu na jednej strane s tradičnými monarchiami a ich centralizovanej moci a na druhej strane so zástupcami krajín, ktorí presadzovali predstavu osamostatnenia spod monarchie a vytvorenie až samostatných štátov v rámci Európy (Lasicová, Ušiak, 2012).

2.2 OBDOBIE PO VESTFÁLSKOM MIERI

Tridsaťročná vojna mala zásadný vplyv na Európu, jej koniec a Vestfálský mier (24.10.1648) znamenal pokrok v chápaní moci. Vznikli suverénne štáty, ktoré svoju suverenitu zakotvili vo svojich zákonoch. V podstate zanikla Svätá rímska ríša a vznikli samostatné mocnosti ako Francúzko, Holandsko, Švédsko. Medzi nevýznamnejšie prínosy vestfálskeho mieru bolo jednoznačne postavenie politicko-diplomatickej sféry pred náboženské záujmy, rešpektovanie zásady štátnej zvrchovanosti (rešpektovanie územnej celistvosti a nevmiešavanie sa do vnútorných záležitostí), vznik decentralizovaného systému suverénnych štátov bez nadradenej autority a vznik oficiálnej diplomacie (Lasicová, Ušiak, 2012). Štáty získali monopol na vedenie vojny.

Ďalším, z pohľadu bezpečnosti v Európe, významným prínosom vestfálskeho mieru, bolo vytvorenie celoeurópskej konferencie pri riešení závažných otázok medzinárodnej politiky a zásad riešenia sporov.

Systém diplomacie a zabezpečovania mieru v tomto období priniesol dva základné princípy, alebo rozmery ako bola vnímaná suverenita v Európe. Za prvé, že všetky štáty si z pohľadu vlastnej suverenity boli rovné. Druhým rozmerom bolo vnímanie vnútornej suverenity štátu, tzn., že každý štát bol zvrchovaný a iný štát nemal právo sa vmiešavať alebo obmedzovať jeho vlastnú správu na území alebo vlastných občanov (Fiala, Pitrová, 2003).

Tento bezpečnostný systém v Európe po roku 1648 sa vyznačoval špecifickým bezpečnostným prostredím, ktoré sa po prvý krát týkalo aj kolónií mimo Európy. Štáty, ktoré mali kolónie, sa snažili prenášať alebo aplikovať európsky bezpečnostný systém aj za vlastnými hranicami, čiže v kolóniách. Európsky bezpečnostný systém naberal globálne rozmery. Vznik medzinárodného práva v tomto období dával možnosť do istej miery ovplyvňovať štáty, ktoré sa vymaňovali z európskeho bezpečnostného systému. Práve diplomacia a medzinárodné právo zohrali veľkú rolu pri určovaní trendov bezpečnosti v Európe. V tomto období si najvyspelejšie štáty začali formovať vlastné bezpečnostné stratégie, ktoré sa prenášali do politiky a tým aj do medzinárodných vzťahov. Takýto bezpečnostný systém sa vyznačoval rovnováhou moci a udržal sa takmer až do konca 2. svetovej vojny (Lasicová, Ušiak, 2012).

2.3 VIEDENSKÝ KONGRES A EURÓPSKY KONCERT

Porevolučné obdobie vo Francúzku (Veľká francúzska revolúcia, roky 1798 - 1799) prinieslo nové hodnoty, ako vnímanie každého človeka v štáte ako občana, ľudské práva, slobody, vlastníctvo, odpor proti útlaku a iné. Na druhej strane toto obdobie bolo charakteristické silnou autoritatívnou vládou Napoleóna, ktorý si dobyvačnými vojnami podmanil takmer celú Európu. Po uzavretí zmluvy s Ruskom (Tylžský mier, 1807) sa Európa bipolarizovala na dve zóny, s francúzskym a ruským vplyvom (Lasicová, Ušiak, 2012).

Bipolaritné rozdelenie Európy sa skončilo porušením tylžského mieru, keď Napoleon viedol masívnu vojenskú kampaň do Ruska. Postupné udalosti v nasledujúcich rokoch mali za následok ukončenia napoleonských vojen (Lasicová, Ušiak, 2012).

Definitívne zavŕšenie napoleonských vojen sa udialo na viedenskom kongrese (1814 - 1815) všetkých európskych štátov, na ktorom boli dohodnuté hranice všetkých zainteresovaných štátov. Mierový kongres priniesol koncepciu rovnováhy síl, ktorá mala zabrániť vzostupu ďalšieho Napoleona a zabezpečiť trvalý mier v Európe. Tento systém sa nazýva aj ako Európsky koncert alebo Koncert veľmocí a mal za úlohy nastoliť a udržať trvalý mier v Európe (Lasicová, Ušiak, 2012).

Európsky koncert umožňoval vznik spojenectiev alebo aliancií. Najvýznamnejšou takouto alianciou bola Svätá aliancia, čiže spolok európskych kresťanských panovníkov (Rusko, Prusko, Rakúsko, a postupne aj ostatné európske štáty, okrem Anglicka, škandinávskych štátov, Turecka a pápeža). Fungovanie spolku bolo založený na princípe takmer neobmedzeného vládnutia panovníka v jednotlivých monarchiách. Hodnoty európskeho koncertu sa mali napĺňať prostredníctvom stretnutí uvedených panovníkov alebo ich ministrov. Ideou bolo spoločne zabraňovať vzniku revolučných hnutí, nedovoliť národné uvedomovanie a takto udržiavať jednotu svojich štátov a tým aj podporovať mier v Európe. V rámci týchto zásad mal spolok právo zasahovať aj do suverenity štátov a tak ovplyvňovať dianie v nich.

Nakoľko Anglicko odmietlo vstup do Svätej aliancie, v európskom koncerte vytváralo dostatočne významného a vojensky silného hráča, ktorý mohol pôsobiť ako mediátor (arbitér, balancér) v sporoch Svätej aliancie a štátu, ktorý bol touto alianciou ovplyvňovaný. Zároveň Anglicko mohlo vstúpiť do sporu za podmienok, že mohlo učiť životne dôležité hodnoty sporu, podľa vlastného uváženia sa mohlo prikloniť a hociktorú stranu a nakoľko disponovalo

výrazným vojenským potenciálom, táto podmienka by bola pre spor rozhodujúca. Preto si Anglicko mohlo dovoliť zvoliť vlastný prospech zo sporu (Fiala, Kutílek, Pitrová, 2018).

2.4 BEZPEČNOSŤ V EURÓPE PO 1. SVETOVEJ VOJNE

Koniec 1. svetovej vojny priniesol nový politický ale aj bezpečnostný systém, ktorý je nazývaný aj ako versaillský (mierový) systém. Tento systém bol výsledkom mierových rokovaní, ktoré sa odohrávali v Paríži (parížska mierová konferencia), na ktorej postupom času v priebehu 6 mesiacov boli podpísané mierové dohody s Nemeckom (Versailles, 28. jún 1919), Rakúskom (Saint-Germain-en-Laye, 10. september 1919), Bulharskom (Neuilly-sur-Seine, 27. november 1919), Maďarskom (Veľký Trianon, 4. jún 1920) a Tureckom (Sèvres,10. august 1920). Podmienky dohôd diktovali víťazné mocnosti, ktoré určili nové hranice Európy a umožnili aj vzniku nových nástupníckych štátov (Fiala, Kutílek, Pitrová, 2018).

Versaillský systém priniesol okrem nového rozdelenia Európy aj novú celosvetovú organizáciu, ktorá sa mala zaoberať najdôležitejšími otázkami medzinárodnej politiky a bezpečnosti vo svete. Tou organizáciou bola Spoločnosť národov (League of Nations) so sídlom v Ženeve. Najväčším iniciátorom jej vzniku bol 28. prezident USA T. W. Wilson. Cieľom Spoločnosti národov bolo udržanie mieru a zabraňovanie konfliktom na celom svete. Pri jej založení v roku 1919 bolo 42 štátov (vrátane Československa), neskôr pristúpilo ďalších 21 štátov.

Bezpečnostný systém pod taktovkou Spoločnosti národov sformoval aj nové bezpečnostné prostredie. Nakoľko podmienky určovali víťazné mocnosti, takéto bezpečnostné prostredie sa vyznačovalo polaritou víťazov a porazených. Toto stotožňovanie bezpečnosti a ovládanie moci viedlo k postupnému nárastu nacionalizmu a fašizmu v porazenom Nemecku a neskôr aj k rozpútaniu 2. svetovej vojny.

2.5 BEZPEČNOSŤ V EURÓPE PO 2. SVETOVEJ VOJNE

Koniec 2. svetovej vojny znova nastolil nový bezpečnostný priestor – bipolárny. Na jednej strane s vplyvom západných víťazných mocností a naproti tomu priestor strednej a východnej Európy s vplyvom ZSSR. Postupimská konferencia a následná konferencia v San Franciscu umožnila vznik organizácie spojených národov (United Nations) a Charty OSN. Tak isto ako v prípade Spoločnosti národov, cieľom OSN bol svetový mier a predchádzanie vojnovým konfliktom vo svete.

Už počas Jaltskej konferencie (Jalta, 4.-11.2.1945) a neskôr počas Postupimskej konferencie (Postupim, 17.7.-2.8.1945) sa ukazovalo, že Európa bude politicky rozdelená, čo neskôr malo aj zásadný vplyv na bezpečnosť nie len v Európe ale aj vo svete. V plnej miere sa prejavili politické a hlavne ideologické nezhody medzi USA a ZSSR, kde medzi sebou súperili demokratické princípy na strane západných víťazných mocnosti a na druhej strane komunistické ideológie. Toto súperenie a vzniknuté napätie dalo impulz pre vznik dvoch bezpečnostných organizácií, a to Severoatlantickej aliancie (North Atlantic Treaty Organization – NATO) a Varšavskej zmluvy. Snahou obidvoch organizácií bola ochrana jedného pred druhým (Lasicová, Ušiak, 2012).

Podľa Trumanovej doktríny bolo hlavnou úlohou zabrániť rozširovaniu komunizmu vo svete. Naopak Brežnevová doktrína hlásala princíp intervencie (aj vojenskej) na udržanie komunistických záujmov vo svojej sfére vplyvu. Na základe tohto princípu vojská Varšavskej zmluvy intervenovali do NDR (1953 a 1961), Maďarska (1956), ČSSR (1968) a do Poľska (1980, 1981 – tu však bez vojenskej účasti) (Lasicová, Ušiak, 2012).

Toto obdobie, nazývané aj ako Studená vojna, prinieslo obrovské preteky v zbrojení. Bezpečnosť vo svete bola neustále na hrane. Situácie, ako zostrelenie amerického špionážneho lietadla nad územím ZSSR a zajatie jeho pilota (F. G. Powersa) v roku 1960, alebo kubánska raketová kríza v roku 1962 prispievali k destabilizácií bezpečnosti a speli k nukleárnej vojne. K stabilizovaniu bezpečnosti dochádza až zo zánikom Varšavskej zmluvy. Následkom geopolitických zmien, ktoré sa odohrali koncom osemdesiatych a začiatkom deväťdesiatych rokov v ZSSR, ako dôsledok jeho liberalizácie, politiky glasnosti a perestrojky M. S. Gorbačova sa v tomto období uvoľnilo striktné vedenie z Moskvy. V plnej miere sa prejavila multietnickosť a separatistické snahy v mnohých jeho republikách. Toto bol impulz na rozpad ZSSR a zánik Varšavskej zmluvy. NATO stratilo svojho najväčšieho oponenta.

2.6 VZNIK EÚ A JEJ BEZPEČNOSŤ

Prakticky najvýznamnejším krokom po skončení 2. svetovej vojny bol Európsky kongres v Haagu (7.5.1948) na ktorom sa zúčastnilo viac ako 700 európskych delegátov. Ústrednou témou bolo zjednotenie kľúčových oblasti suverenít európskych štátov. Výsledkom konferencie boli Politické prehlásenia, Európske a sociálne prehlásenia a Správa Európanom. Jednalo sa o dokumenty, na základe ktorých bolo možné neskôr vytvoriť Chartu ľudských práv a slobôd a aj samotnú Európsku radu (Fiala, Kutílek, Pitrová, 2018). Práve charta je dodnes najvýznamnejším európskym dokumentom, ktorý má Európanom garantovať bezpečnosť (Fiala, Kutílek, Pitrová, 2018).

Povojnové roky však neboli naklonené urýchlenému zjednoteniu Európy, nakoľko jednotlivé štáty si po získaní vlastnej slobody znovu utvárali vlastnú suverenitu a zvrchovanosť. Nebola dostatočná vôľa na odovzdanie časti suverenity do správy niekomu inému a významný vplyv na zjednocovanie mala aj vyššie popisovaná bipolarita Európy (hlavne komunisticky orientovaná stredná a východná Európa).

Európska Rada (tvorená ministrami zahraničných vecí) vznikla ako konsenzus medzi možnosťou nejednotnej Európy na jednej strane a na druhej strane s centrálnym riadením jednotnej Európy. Takýto model pripúšťal inštitút zhromaždenia zástupcov vlád, ktorí budú prerokovávať návrhy a vypracovávať odporúčania pre Európsku radu, ktorá bude mať rozhodujúcu právomoc.

V povojnovom období, hlavne v západnej Európe dochádza k úzkej spolupráci medzi niektorými štátmi. Výsledkom tejto úzkej spolupráce v regióne bol vznik Európskeho spoločenstva pre uhlie a oceľ. V rámci tohto spoločenstva bolo do povojnovej obnovy ekonomiky zapojené aj Západné Nemecko, ktoré takto deklarovalo spoluprácu v rámci západnej Európy. Naproti tomu Anglicko sa vybralo cestou spolupráce s USA. Napriek týmto zjednocujúcim snahám hrozba komunizmu pretrvávala a odpoveďou mala byť spoločná európska armáda. Hlavným propagátorom bolo Francúzsko, ktoré sa naďalej obávalo agresie zo strany Nemecka. Táto obava bola hlavným iniciátorom vzniku spoločného európskeho vojska, ktoré by podliehalo spoločnému európskemu veleniu (Fiala, Kutílek, Pitrová, 2018). Zmluva o Európskom obrannom spoločenstve bola podpísaná 27.5.1952. Jej ratifikácia by znamenala riešenie pre zabezpečenie európskej bezpečnosti prostredníctvom európskej armády. Avšak ratifikácia neprebehla úspešne, nakoľko francúzska vláda tento dokument odmietla a tým znemožnila vznik európskej armády. Otázky európskej bezpečnosti boli znovu otvorené. Čiastočne ich vyriešila Západoeurópska únia (6.5.1955), ktorá vzišla z návrhu počas Parížskej konferencie konanej rok pred tým. Západoeurópska únia oficiálne ukončila okupáciu Nemecka a umožnila jeho vstup do NATO s čím súhlasilo aj Francúzsko (Fiala, Kutílek, Pitrová, 2018).

Séria udalostí a politických zmien v Európe i vo svete, ako pád Berlínskeho múra, okupácia Kuvajtu a následná vojenská operácia Púštna búrka, konflikt v Juhoslávii znova koncom 80-tých a začiatkom 90-tých rokov nastolili požiadavky bezpečnosti v Európe.

Európska únia vznikla 1. novembra 1993, po sérií medzivládnych rokovaní, kde na poslednom z nich v holandskom Maastrichte (9.-10.12.1991) bola predložená Zmluva o Európskej Únií. Maastrichtská zmluva bola postavená na koncepcií troch pilierov, ktoré mali zabezpečiť mechanizmus prijímaní spoločných rozhodovaní. Jednotlivé oblasti spoločných politík boli rozdelené do troch oblastí. Oblasť bezpečnosti Európskej únie a jej občanov bol obsahom 2. piliera s názvom Spoločná zahraničná a bezpečnostná politika (Fiala, Kutílek, Pitrová, 2018).

Cieľom Spoločnej zahraničnej a bezpečnostnej politiky (SZBP) je riešiť konflikty a podporovať medzinárodné porozumenie. Tento cieľ má byť napĺňaný prostredníctvom diplomacie a dodržiavaním medzinárodných pravidiel. „*Hlavnou úlohou zahraničnej a bezpečnostnej politiky EÚ je: ochrana mieru, posilnenie medzinárodnej bezpečnosti, podpora medzinárodnej spolupráce, rozvoj a upevňovanie demokracie a právneho štátu a dodržiavanie ľudských práv a základných slobôd*“ (Európska únia, 2021).

3 VÝVOJ VNÚTORNEJ BEZPEČNOSTI V EÚ

Vnútornú bezpečnosť EÚ je nutné chápať ako široký a komplexný koncept, ktorý zahŕňa viacero odvetví, s cieľom riešiť hrozby, ktoré majú priamy vplyv na bezpečnosť občanov v EÚ (Európska únia, 2010). Nakoľko sa jedná o vnútornú bezpečnosť EÚ, čiže spoločenstvo viacerých európskych krajín, tak na zabezpečovaní tejto bezpečnosti musia spolupracovať všetky krajiny. Z princípu vylúčenia jednotného právneho aktu (EUR-Lex, 2012) nebolo možné prijať jednotnú direktívu platnú pre všetky krajiny EÚ. Preto je nutná spolupráca a hlavne poskytovanie a výmena informácií medzi jednotlivými štátmi EÚ.

V 70-tých rokoch výrazne narástli teroristické útoky (hlavne únosy civilných lietadiel). V reakcií na tieto činy bolo v tých rokoch prijatých niekoľko medzinárodných zmlúv, ktoré podporovali boj proti terorizmu. Napríklad: dohovor o potlačení protiprávneho zmocnenia sa lietadiel (ASPI, 1974), medzinárodný dohovor proti braniu rukojemníka (1988), dohovor o zabránení a trestaní trestných činov proti osobám požívajúcim medzinárodnú ochranu, včítane diplomatických zástupcov (Slov-Lex, 1978) a mnoho iných.

Vo vtedajšom Európskom spoločenstve, na úrovni ministerstiev vnútra a spravodlivosti, vznikla medzivládna skupina s názvom TREVI (Terrorisme, Radicalisme, Extremisme, Violence Internationale - súčasný EUROPOL). Jej účelom bolo zabezpečovanie výmeny informácií medzi spravodajskými službami, stanovovanie spoločnej metodiky pre postup v prípade teroristických činov, koordinovanie boja s terorizmom (Euroskop, 2018). Neskôr TREVI svoje zameranie okrem terorizmu rozšírila aj na oblasti cezhraničnej trestnej činnosti v rámci európskeho spoločenstva.

3.1 AMSTERDAMSKÁ ZMLUVA

Spolupráca v oblasti bezpečnosti medzi členskými štátmi EÚ bola riadne zakomponovaná už v Maastrichtskej zmluve (2. pilier – Spoločná zahraničná bezpečnostná politika) (Fiala, Kutílek, Pitrová, 2018). Prijatím Amsterdamskej zmluvy (revízia Zmluvy o EÚ ako výsledok medzivládnej konferencie v roku 1996 v Turíne, následné ratifikovanie prebehlo 2.10.1997 v Amsterdame) si EÚ stanovila zachovať a rozvíjať úniu ako priestor slobody, bezpečnosti a práva, v ktorom je zaručený voľný pohyb osôb spolu s príslušnými opatreniami týkajúcich sa ochrany vonkajších hraníc, azylu, prisťahovalectva, prevencie a boja proti zločinu (Amsterdamská zmluva, 1997).

3.2 VIEDENSKÝ AKČNÝ PLÁN

Ďalším krokom k zabezpečeniu vnútornej bezpečnosti EÚ je tzv. Viedenský akčný plán. Jeho úlohou bolo zabezpečiť realizáciu prioritných úloh Amsterdamskej zmluvy v čo najkratšom čase (Európska únia, 1998). Tým by bol naplnený hlavný cieľ Amsterdamskej zmluvy: zachovať a rozvíjať úniu ako priestor slobody, bezpečnosti a práva, v ktorom je zaručený voľný pohyb osôb.

3.3 TAMPERSKÝ PROGRAM

Už v októbri 1999 na Viedenský akčný plán bezprostredne nadviazal tzv. Tamperský program. „*Postupné zriadenie územia slobody, bezpečnosti a spravodlivosti bolo novým cieľom Európskej únie po uzatvorení Amsterdamskej dohody. Európska rada, ktorá zasadala v októbri 1999 v Tampere, zaradila tento cieľ na prvé miesto politického programu Únie a stanovila veľmi ambiciózny program. Tento program podrobne určuje orientácie danej politiky, ako i konkrétne ciele s časovým harmonogramom. Komisia vypracovala na žiadosť Európskej rady prehľad, na základe ktorého sa bude každý polrok sledovať dosiahnutý pokrok.*“ (Eur-Lex, 2004, s. 1)

3.4 EURÓPSKA BEZPEČNOSTNÁ STRATÉGIA

Európska bezpečnostná stratégia bola prijatá Radou v decembri 2003. Prvýkrát tak boli ustanovené zásady a vymedzenia jednoznačných cieľov presadzovania bezpečnostných záujmov EÚ a zahŕňala komplexný prístup (Korba, s.a.). V roku 2009 už EÚ nevníma zahraničnú politiku a obranu najmä cez prizmu vzťahov medzi EÚ a USA. Najviditeľnejšou zmenou v bezpečnostnom prostredí Európy je od roku 2003 návrat ohrození z východu. Konkrétne ekonomické a vojenské oživenie Ruska a jeho rastúci príklon k agresívnemu nacionalizmu. To ale neznamená, že novoprijatá bezpečnostná stratégia je len o Rusku, ale tieto aspekty museli byť zohľadnené ako jedna z nových výziev pre európsku bezpečnosť. Značne silnel tlak zo strany NATO na plnenie si záväzkov od členských štátov. EÚ sa spoliehala najmä na obrannú záštitu zo strany NATO, ale zároveň sa vynárala otázka, že ak členské štáty budú viac prispievať na obranu v rámci NATO, zostane im menej prostriedkov na plnenie si záväzkov vyplývajúcich z členstva v EÚ. Nová stratégia mala viac zosúladiť vojenské požiadavky NATO a EÚ (Euroaktív, 2008).

3.5 HAAGSKY PROGRAM

V novembri 2004 Európska rada prijala program na obdobie nasledujúcich piatich rokov (Haagsky program, 2005). Svojím obsahom reagoval na teroristické útoky z 11.9.2001, ale zaoberal sa aj otázkami základných práv a občianstva, azylu, imigrácie a riadenia hraníc, boja proti organizovanej trestnej činnosti, súdnej a policajnej spolupráce (Pikna, 2006).

3.6 ŠTOKHOLMSKÝ PROGRAM

Konkrétne návrhy zamerané na dosiahnutie výhod vyplývajúcich zo spoločného európskeho priestoru priniesol v roku 2009 Štokholmský program. Bol zameraný na politické priority a nástroje pre občanov v priestore slobody, bezpečnosti a spravodlivosti, podporu občianskych práv, uľahčenie života občanov EÚ, Európu ako ochrancu, integrované riadenie vonkajších hraníc, vízovú politiku, dynamickú a komplexnú migračnú politiku, vonkajší rozmer slobody, bezpečnosti a spravodlivosti a iné. Ustanovoval priority EÚ na obdobie 2010 – 2014.

V nadväznosti na úspechy predchádzajúcich programov (Tampereský a Haagsky program) si kladie za cieľ reagovať na budúce úlohy. Ďalšou ambíciou bolo posilňovanie priestoru spravodlivosti, slobody a bezpečnosti pomocou opatrení zameraných na záujmy a potreby občanov. Štokholmský program sa sústreďoval na tieto priority s cieľom vytvoriť bezpečnú Európu, kde sa dodržiavajú základné práva a slobody občanov (Eur-Lex, 2010).

3.7 LISABONSKÁ ZMLUVA

Lisabonská zmluva nadobúda platnosť koncom roka 2009 a priniesla Európskemu parlamentu nové zákonodarné právomoci, čím sa Parlament ocitol pri rozhodovaní o tom, čo EÚ robí a na čo míňa peniaze, na rovnakej úrovni s Radou ministrov. Zmluva takisto zmenila spôsob, akým Parlament spolupracuje s ostatnými inštitúciami, a zvýšila vplyv poslancov pri rozhodovaní o tom, kto povedie EÚ. Tieto reformy priniesli aj zrušenie troch pilierov EÚ a posilnili viaceré inštitúcie pre zahraničnú politiku (napr. zmena funkcie vysokého predstaviteľa pre spoločnú zahraničnú a bezpečnostnú politiku na vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku).

Na týchto základoch v roku 2010 vzniká Stratégia vnútornej bezpečnosti EÚ.

4 STRATÉGIA VNÚTORNEJ BEZPEČNOSTI EURÓPSKEJ ÚNIE: SMEROM K EURÓPSKEMU BEZPEČNOSTNÉMU MODELU

Maastrichtská, Amsterdamská alebo aj Lisabonská zmluva a jednotlivé programy na zabezpečovanie európskej bezpečnosti vytvorili základné podmienky pre to aby sa Európa mohla stať pre svojich občanov priestorom slobody, bezpečnosti a spravodlivosti.

Európska bezpečnostná stratégia bola doplnená v roku 2010 o Stratégia vnútornej bezpečnosti európskej únie: smerom k európskemu bezpečnostnému modelu (Európska únia, 2010). Nová stratégia vnútornej bezpečnosti zdôrazňuje, že „*bezpečnosť je pre občanov Európskej únie jednou z hlavných priorít. Viacročné pracovné programy EÚ už v súčasnosti poskytujú dobrý pragmatický základ pre posilnenie operačnej spolupráce, ale teraz sa vyžaduje širší konsenzus na vízii, hodnotách a cieľoch, na ktorých stojí vnútorná bezpečnosť EÚ*“ (Európska únia, 2010, s. 7).

Je dôležité, aby prijatá stratégia bola schopná sa prispôsobovať občanom, ale i bezpečnostným hrozbám v podobe terorizmu, závažnej a organizovanej trestnej činnosti, obchodovania s drogami, počítačovej kriminality, obchodovania s ľuďmi, sexuálneho vykorisťovania detí a detskej pornografie, hospodárskej trestnej činnosti a korupcii, obchodovania so zbraňami a cezhraničnej trestnej činnosť (Stratégia vnútornej bezpečnosti EU, 2010). K tomu je nutné pripočítať aj katastrofy technogénneho alebo prírodného charakteru a hrozby vyplývajúce zo zvyšovania environmentálnej záťaže nevynímajúc. Stratégia si ale nekladie za cieľ vytvárať nové právomoci. Naopak, má vytvárať predpoklady pre integráciu už existujúcich programov (Štokholmsky program) a bezpečnostných politík jednotlivých členských štátov. Vytvárať predpoklady pre spoluprácu orgánov na presadzovanie práva, justície, colných úradov, pohraničnej stráže a iných orgánov.

Vnútorná bezpečnosť v EÚ je zameraná na ochranu svojich občanov, tzn. chce im poskytnúť pocit bezpečia a ochrany, a to nie len na svojom území ale aj na územiach tretích krajín. Z bezpečnostného prostredia sa nevyníma ani kybernetický priestor. Zabezpečiť ochranu pre ľudí predstavuje pre EÚ mimoriadnu výzvu, preto stratégia vnútornej bezpečnosti:

- „*predostiera spoločné hrozby a výzvy, ktorým čelíme, v dôsledku ktorých je ešte dôležitejšie, aby členské štáty a inštitúcie EÚ spolupracovali na riešení nových výziev, ktoré idú nad rámec našej vnútroštátnej, bilaterálnej či regionálnej spôsobilosti*“;

- „*ustanovuje spoločnú politiku vnútornej bezpečnosti EÚ – a zásady, na ktorých stojí – komplexným a transparentným spôsobom*“;
- „*vymedzuje európsky bezpečnostný model*“ (Európska únia, 2010, s. 12).

4.1 HLAVNÉ VÝZVY PRE VNÚTORNÚ BEZPEČNOSŤ EÚ

Súčasné vonkajšie ale aj vnútorné bezpečnostné prostredie je charakteristické ťažko predvídateľnými hrozbami. Je nutné ich neustále vyhodnocovať a prijímať voči ním adekvátne opatrenia (Bartoš, 2020). EÚ sa v dnešných časoch neistoty snaží za použitia všetkých dostupných prostriedkov zaručiť bezpečnosť v Európe. Preto stratégia za najnaliehavejšie výzvy v oblasti bezpečnosti pre EÚ definuje niekoľko významných spoločných hrozieb ako:
- „*terorizmus*“,
- „*závažná organizovaná trestná činnosť*“,
- „*počítačová kriminalita*“,
- „*cezhraničná trestná činnosť*“,
- „*samotné násilie*“,
- „*prírodné katastrofy a katastrofy spôsobené ľudskou činnosťou*“ (Európska únia, 2010, s. 13-15).

4.1.1 TERORIZMUS

„*V akejkoľvek forme absolútne neberie ohľad na ľudský život a demokratické hodnoty. Jeho globálny dosah, jeho ničivé následky, jeho schopnosť získavať stúpencov prostredníctvom radikalizácie a šírenia propagandy cez internet a rôzne spôsoby financovania spôsobujú, že terorizmus je významnou a stále sa vyvíjajúcou hrozbou pre našu bezpečnosť*“ (Európska únia, 2010, s. 13).

4.1.2 ZÁVAŽNÁ ORGANIZOVANÁ TRESTNÁ ČINNOSŤ

„*V rôznych formách sa objavuje všade tam, kde môže dosiahnuť čo najväčší finančný prospech s čo najmenším rizikom bez ohľadu na hranice. Obchodovanie s drogami, hospodárska trestná činnosť, obchodovanie s ľuďmi, pašovanie ľudí, obchodovanie so zbraňami, sexuálne vykorisťovanie detí a detská pornografia, násilná trestná činnosť, legalizácia príjmov z trestnej činnosti a falšovanie dokladov sú len niektoré zo spôsobov, ktorými sa prejavuje organizovaná a závažná trestná činnosť v EÚ. Navyše korupcia ohrozuje samotné základy demokratického systému a právny štát*“ (Európska únia, 2010, s. 14).

4.1.3 POČÍTAČOVÁ KRIMINALITA

„*Predstavuje globálnu, technickú, cezhraničnú a anonymnú hrozbu pre naše informačné systémy, a preto stavia orgány presadzovania práva pred mnohé ďalšie výzvy*“ (Európska únia, 2010, s. 14). Počítačová kriminalita nepredstavuje hrozbu iba pre občanov EÚ samotných ale aj pre jej ekonomiku. Ročne to predstavuje až niekoľko miliárd euro. Správa o bezpečnosti Slovenskej republiky za rok 2021 (Kancelária bezpečnostnej rady SR, 2021) uvádza, že okrem útokov na kritickú infraštruktúru a dezin boli zaznamenané útoky orientované na krádeže osobných údajov a vydieranie. Prostriedkami útokov boli phishingové kampane, šírenie ransomvéru alebo iného škodlivého kódu. Vzhľadom na neustály nárast trestných činov páchaných v internetovom prostredí v ostatných rokoch vytvorila Európska komisia koordinovanú politiku v úzkej spolupráci členských štátov Európskej únie ako aj ďalších inštitúcií EÚ.

4.1.4 CEZHRANIČNÁ TRESTNÁ ČINNOSŤ

„*Je menej závažná alebo majetková trestná činnosť, často páchaná zločineckými skupinami, má významný vplyv na každodenný život ľudí v Európe*“ (Európska únia, 2010, s. 14).

4.1.5 SAMOTNÉ NÁSILIE

„*Je násilie medzi mladými ľuďmi alebo násilie spojené so športovými podujatiami, ešte zvyšuje škody spôsobené trestnou činnosťou a môže významne poškodiť našu spoločnosť*“ (Európska únia, 2010, s. 14).

4.1.6 PRÍRODNÉ KATASTROFY A KATASTROFY SPÔSOBENÉ ĽUDSKOU ČINNOSŤOU

„*Sú to lesné požiare, zemetrasenia, povodne a búrky, suchá, výpadky v dodávkach energie a významné poruchy informačných a komunikačných technológií. V našej dobe systémy civilnej ochrany predstavujú významný prvok akéhokoľvek moderného bezpečnostného systému*“ (Európska únia, 2010, s. 15).

4.2 REAKCIA NA HLAVNÉ VÝZVY PRE VNÚTORNÚ BEZPEČNOSŤ EÚ

Ako už bolo uvádzané, každý členský štát si vytvára vlastné mechanizmy ako reagovať a pôsobiť proti týmto hrozbám. Stratégia vnútornej bezpečnosti ale ponúka spoločné možnosti ako sa vysporiadať so spoločnými hrozbami. Najmä preto, že zločinecké skupiny nerešpektujú žiadne hranice, je nutná spolupráca orgánov jednotlivých štátov a jednotný spoločný prístup z úrovne EÚ (Európska únia, 2010). Znova je nutné pripomenúť nemožnosť prijať jednotnú direktívu platnú pre všetky krajiny EÚ, preto je zavedenie jednotných postupov a spolupráca na európskej (ale aj svetovej) úrovni viac ako nevyhnutná.

EÚ v tejto oblasti za posledné roky dosiahla významný pokrok. Od odstránenia kontrol na vnútorných hraniciach, ktoré umožňujú voľný pohyb ľudí v rámci schengenského priestoru, je napríklad veľmi dôležitá zvýšená spolupráca v oblasti presadzovania práva a justičná spolupráca. Takmer vo všetkých oblastiach spolupráce boli zavedené nástroje na spoluprácu a výmenu informácií, ako napr.:

- „***analýza budúcich situácií a scenárov***: *predpovedanie hrozieb. Europol a iné agentúry EÚ vydávajú pravidelné posúdenia hrozieb*“
- „***náležitá reakcia: plánovanie, programovanie a riešenie následkov***. *Boli vypracované pracovné programy, ktoré nám umožňujú metodicky riešiť nebezpečenstvá pre občanov a ich obavy. Stratégie a osobitné pracovné plány sa vypracovali i v oblastiach boja proti terorizmu, pašovania drog, pašovania ľudí, organizovanej trestnej činnosti a civilnej ochrany. Okrem toho mechanizmus civilnej ochrany Spoločenstva koordinuje reakciu členských štátov na prírodné katastrofy a katastrofy spôsobené ľudskou činnosťou*“
- „***účinnosť v praxi: práca agentúr, inštitúcií a orgánov***. *Bolo vytvorených niekoľko agentúr osobitne v rámci EÚ a tieto zahŕňajú: Europol, ktorého hlavnými cieľmi sú zber a výmena informácií a uľahčovanie spolupráce medzi orgánmi presadzovania práva v ich boji proti organizovanej trestnej činnosti a terorizmu, Eurojust, ktorý má za úlohu koordináciu a zvyšovanie účinnosti justičných orgánov a Frontex, ktorý riadi operačnú spoluprácu na vonkajších hraniciach. EÚ taktiež vytvorila funkciu koordinátora pre boj proti terorizmu. Tiež sa zriadili iné orgány a siete v oblastiach odbornej prípravy, boja proti drogám, predchádzania trestnej činnosti, boja proti korupcii a justičnej spolupráce v trestných veciach*“

- „***nástroje založené na vzájomnom uznávaní, na účely výmeny informácií a na uľahčenie spoločných vyšetrovaní a operácií***. *Nástroje založené na vzájomnom uznávaní zahŕňajú európsky zatykač a ustanovenia na zmrazenie aktív. Vytvorili sa tiež databázy, ako je Schengenský informačný systém a siete na výmenu informácií o registroch trestov, o boji proti násilí spojenom so športovými podujatiami, o hľadaných osobách alebo odcudzených vozidlách a o vydaných alebo zamietnutých vízach. Využívanie údajov o DNA a odtlačkoch prstov pomáha identifikovať anonymné stopy na miestach činu. Právne nástroje EÚ uľahčujú operačnú spoluprácu medzi členskými štátmi, ako je zriaďovanie spoločných vyšetrovacích tímov, organizovanie spoločných operácií a úzka spolupráca, aby sa zabezpečila bezpečnosť medzinárodných podujatí, vrátane významných športových súťaží*“
- „***na účely hodnotenia účinnosti našej činnosti sa vyvinuli mechanizmy hodnotenia***. *Napr. využívanie partnerského hodnotenia v oblasti boja proti terorizmu a organizovanej trestnej činnosti, ktoré prispelo k zlepšeniu vzájomnej dôvery*“ (Európska únia, 2010, s. 16-18).

Realizácia budúcich operácií EÚ v oblasti vnútornej bezpečnosti bude záležať na dvoch faktoroch, a to politickej vôli a spôsobilostiach a štruktúrach na boj s aktuálnymi hrozbami členských štátov. Bezpečnostné prostredie EÚ, ktoré je závislé od mieru a stability v jej susedstve, je nestálejšie, nepredvídateľnejšie, zložitejšie a citlivejšie na vonkajší tlak, ktorý sa už vyvíja formou hybridnej vojny, vrátane nepriateľskej propagandy zo strany Ruska a iných aktérov a navyše dochádza k nárastu hrozieb zo strany radikálnych teroristických skupín, ktoré bránia EÚ v uplatňovaní jej zvrchovanosti a strategickej autonómie je v tomto čase nesmierne zložité zabezpečovať. Prejavuje sa nestabilita a nepredvídateľnosť na hraniciach EÚ a v jej blízkom susedstve. To predstavuje priamu hrozbu pre bezpečnosť EÚ (Európsky parlament, 2020).

ZÁVER

Cieľom príspevku bolo analyzovať príčiny vzniku potreby zaoberať sa vnútornou bezpečnosťou EÚ a vytvoriť historický prehľad jej vývoja. Príspevok objasnil zameranie dokumentu Stratégia vnútornej bezpečnosti EÚ a priblížil najväčšie hrozby vnútenej bezpečnosti EÚ. Čiastočne sa dotýkal vnútorného bezpečnostného prostredia EÚ a stručne previedol vznikom Európskej únie.

„*Európski občania majú všade v Európskej únii nárok na slobodný život bez strachu pred prenasledovaním alebo násilím*“ (Fontaine, 2010, s. 59). Vo vnútri schengenského priestoru nejestvujú hraničné kontroly, EÚ prijala rôzne opatrenia a politiky na zabezpečovanie vlastnej vnútornej bezpečnosti. Ich cieľom je vytvoriť spoluprácu v oblasti vnútornej bezpečnosti EÚ, reagovať na meniace sa bezpečnostné výzvy a využiť potenciál technologického vývoja, spolupráca v oblasti presadzovania práva, udržanie tempa s technologickým pokrokom, globálna spolupráca, boj proti nadnárodnej organizovanej trestnej činnosti, predchádzanie terorizmu a boj proti nemu (Európska rada, 2020). Členstvo v EÚ preto poskytuje medzinárodnú garanciu obrany a umožňuje dosahovanie spoločných bezpečnostných cieľov pri formovaní bezpečnostného prostredia každého členského štátu (Kompan, 2019). Od svojho vzniku EÚ neustále preukazuje dôležitosť európskej jednoty aj v oblasti bezpečnosti. Vývoj a progres v oblasti spoločnej bezpečnosti predstavujú aj spoločné dokumenty, ako napr. Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie z roku 2020 alebo aktuálny Strategický kompas pre bezpečnosť a obranu z roku 2022 (Rada európskej únie, 2022).

Medzinárodný zločin, terorizmus a hrozby z kybernetického priestoru však napriek tomu patria medzi hlavné obavy Európanov. Je jasné, že aj pri slobode pohybu kdekoľvek v EÚ musí byť zabezpečená rovnaká ochrana a prístup k spravodlivosti. Takto sa postupne z EÚ stáva jednotný priestor slobody, bezpečnosti a spravodlivosti (Fontaine, 2010). Z analýzy

dokumentov týkajúcich sa vnútornej bezpečnosti vyplýva, že v súčasnej dobe je prvoradou výzvou pre bezpečnosť EÚ kybernetická bezpečnosť. Táto oblasť je takmer vo všetkých bezpečnostných dokumentoch EÚ na prvoradom mieste. Druhou, nie menej podstatnou výzvou je nelegálna migrácia. Od februára 2022 sa nejedná už striktne iba o nelegálnu migráciu. Konflikt na Ukrajine zapríčinil masový útek obyvateľstva zo zón postihnutých konfliktom smerom do EÚ. EÚ sa k tejto výzve postavilo zodpovedne a prostredníctvom nie len susedných štátov ako Slovensko, Poľsko, Maďarsko, Rumunsko, ktoré sú návalom migrantov najviac postihnuté, poskytlo potrebnú pomoc a humanitárnu pomoc a tým prispieva spoločnej bezpečnosti v EÚ.

„*Európska únia sa vo všeobecnosti považuje za jedno z najbezpečnejších miest aj v dnešnom čoraz nepokojnejšom svete. Nemožno to však považovať za samozrejmosť*.“ (Eur-Lex, 2020, s. 29) Jednotný, slobodný, bezpečný a spravodlivý priestor by nebol možný bez vytvorenia Európskej únie. Únia vznikla na základe zmlúv, v ktorých je európska bezpečnosť riadne zakotvená. Samotné zmluvy však nie sú garanciou bezpečnosti. Bezpečnosť je treba budovať a ochraňovať. K tomu Európska rada prijala viacero politík a programov. Z pohľadu vnútornej bezpečnosti EÚ to sú Tamperský program (1999 – 2004), Haagsky program (2005 – 2009) a Štokholmský program (2010 – 2014).

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ASPI. 1974. *Dohovor o potlačení protiprávneho zmocnenia sa lietadiel.* [online]. [cit. 2022-06-14]. Dostupné na URL: <https://lnk.sk/qgiy>.

BARTOŠ, M. 2020. *Taktická úloha kontrola a ovládanie davu.* In: Vojenské reflexie 2020: ročník 15, číslo 2/20. Liptovský Mikuláš: Akadémia ozbrojených síl generála M.R. Štefánika, 2020. s. 210-222. ISSN 1336-9202.

BREZULA, J. 2020. *Obranná politika štátu a jej zameranie v podmienkach Slovenskej republiky*. In: Security Forum 2020. Banská Bystrica: Interpolis, 2020. s. 18 - 29. ISBN 978-80-973394-2-5.

EUROAKTÍV. 2008. [online]. [cit. 2022-06-17]. Dostupné na URL: < https://lnk.sk/hoxt>.

EURÓPSKA RADA. 2020. *Závery rady o vnútornej bezpečnosti a európskom policajnom partnerstve*. [online]. [cit. 2022-06-05]. Dostupné na URL:<https://lnk.sk/ipsr>.

EURÓPSKA ÚNIA. 1998. *Akčný plán rady a komisie o tom, ako najlepšie vykonávať ustanovenia amsterdamskej zmluvy v oblasti slobody, bezpečnosti a spravodlivosti (Viedenský akčný plán).* [online]. [cit. 2022-06-15]. Dostupné na URL: <https://lnk.sk/lsy6>.

EURÓPSKA ÚNIA. 2010. *Stratégia vnútornej bezpečnosti európskej únie: smerom k európskemu bezpečnostnému modelu.* Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2010. 33 s. ISBN 978-92-824-2691-3.

EURÓPSKA ÚNIA. 2021. *Zahraničná a bezpečnostná politika*. 2021. [online]. [cit. 2022-06-14]. Dostupné na URL: <https://lnk.sk/zp38>.

EURÓPSKY PARLAMENT. 2020. *Výročná správa o vykonávaní spoločnej zahraničnej a bezpečnostnej politiky*. [online]. [cit. 2022-06-16]. Dostupné na URL: <https://lnk.sk/ehxm>.

EUR-LEX. 1951. *Zmluva o založení európskeho spoločenstva uhlia a ocele, zmluva o esuo.* [online]. [cit. 2022-06-05]. Dostupné na URL: <https://lnk.sk/iity>.

EUR-LEX. 2004. *Oznámenie komisie rade a európskemu parlamentu - územie slobody, bezpečnosti a spravodlivosti : bilancia tamperského programu a perspektívy.* [online]. [cit. 2022-06-16]. Dostupné na URL: <https://lnk.sk/lrc6>.

EUR-LEX. 2010. *Štokholmský program – otvorená a bezpečná Európa, ktorá slúži občanom a chráni ich*. [online]. [cit. 2022-06-16]. Dostupné na URL: <https://lnk.sk/dvam>.

EUR-LEX. 2012. *Zmluva o európskej únii (konsilidované znenie)*. [online]. [cit. 2022-06-05]. Dostupné na URL:<https://lnk.sk/hqtv>.

EUR-LEX. 2020. *O stratégii EÚ pre bezpečnostnú úniu*. [online]. [cit. 2022-09-19]. Dostupné na URL:<https://lnk.sk/x023>.

EUROSKOP. 2018. [online]. [cit. 2022-06-16]. Dostupné na URL: < https://lnk.sk/vxdg>.

FIALA, P. – PITROVÁ, M. 2003. *Európská unie*. 1. vydanie. Brno : Centrum pro studium demokracie a kultúry, 2003. 743 s. ISBN 80-7325-015-2.

FIALA, P. – KUTÍLEK, O. – PITROVÁ, M. 2018. *Európská unie*. 3. vydanie. Brno : Centrum pro studium demokracie a kultúry, 2003. 997 s. ISBN 9788073254506.

FONTAINE, P. 2010. *Európa v 12 lekciách*. Luxemburg :Úrad pre vydávanie publikácií Európskej únie, 2010. 80 s. ISBN 978-92-79-17498-8.

FURNESS, M. – SCHÄFER, I. 2015. *The 2015 European neighbourhood policy review: more realism, less ambition*. [online]. [cit. 2022-06-05]. Dostupné na URL: < https://lnk.sk/jdv7>.

HAAGSKY PROGRAM. 2005. [online]. [cit. 2022-06-16]. Dostupné na URL:<https://lnk.sk/lfmz>.

HOFREITER, L. 2016. *Bezpečnostné prostredie súčasného sveta*. Zlín : Radim Bačuvčík - VeRBuM, 2016. 160 s. ISBN 978-80-87500-79-8.

KANCELÁRIA BEZPEČNOSTNEJ RADY SR, 2021. *Správa o bezpečnosti Slovenskej republiky za rok 2021*. [online]. [cit. 2022-06-16]. Dostupné na URL: <https://lnk.sk/ipbz>.

KOMPAN, J. 2020. *Using the SWOT analysis of the external security of the Slovak republic as a basis for defense planning.* In: SECURITY FORUM 2019: 12th Annual International Scientific Conference Proceedings. Banská Bystrica: Univerzita Mateja Bela, 2019, s.59-66. ISBN 978-80-973394-1-8.

KORBA,M. s.a. *Európska bezpečnostná a obranná politika a jej limity*. [online]. [cit. 2022-06-16]. Dostupné na URL: <https://lnk.sk/htwu>.

LAML, R. 2014. *K problematike ponímania bezpečnostného prostredia*. [online]. [cit. 2022-06-06]. Dostupné na URL: <https://lnk.sk/xfkv>.

LASICOVÁ, J. - UŠIAK, J. 2012. *Bezpečnosť ako kategória*. Bratislava : VEDA, Vydavateľstvo Slovenskej akadémie vied, 2012. 264 s. ISBN 978-80-224-1284-1.

Národná rada SR. 1997. *Amsterdamská zmluva, ktorá mení zmluvu o európskej únii, zmluvy o založení európskych spoločenstiev a niektoré súvisiace akty.* [online]. [cit. 2022-06-15]. Dostupné na URL: <https://lnk.sk/aha1>.

PIKNA, B. 2006. *Mezinárodní terorismus a bezpečnost Europské únie – právní náhled*. Praha : Linde. 2006. 408 s. ISBN 80-7201-615-6.

PORADA, V. a kol. 2019. *Bezpečnostní vědy*. Plzeň : Aleš Čeněk. 2019. 784 s. ISBN 978-80-7380-758-0.

RADA EURÓPSKEJ ÚNIE. 2022. *Strategický kompas pre bezpečnosť a obranu.* [online]. [cit. 2022-06-05]. Dostupné na URL:<https://lnk.sk/iph0>

SLOV-LEX. 1978. *Dohovor o zabránení a trestaní trestných činov proti osobám požívajúcim medzinárodnú ochranu, včítane diplomatických zástupcov*. [online]. [cit. 2022-06-14]. Dostupné na URL: <https://lnk.sk/hdpz>.

SLOV-LEX. 1988. *Medzinárodný dohovor proti braniu rukojemníka*. [online]. [cit. 2022-06-15]. Dostupné na URL: <https://lnk.sk/iqta>.

S&D. s. a. *Vnútorná bezpečnosť*. [online]. [cit. 2022-06-05]. Dostupné na URL: <https://lnk.sk/bqi5>.

TURAJ, M. 2021. *O potrebe ozbrojených síl Európskej únie reprezentovaných bojovými skupinami Európskej únie*. In: Národná a medzinárodná bezpečnosť 2021, Zborník príspevkov z medzinárodnej vedeckej konferencie. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2021. s. 430-440. ISBN 978-80-8040-606-6.

TVARUŠKA, P. 2018. *Možnosti využitia scenárov v teórií bezpečnostných štúdií*. In: Vojenské reflexie 2019: ročník 13, číslo 2/18. Liptovský Mikuláš: Akadémia ozbrojených síl generála M.R. Štefánika, 2018. s. 21-33. ISSN 1336-9202.

mjr. Ing. Miroslav MUŠINKA
doktorand externého štúdia Katedry bezpečnosti a obrany,
Katedra vojenskej taktiky a operačného umenia, Akadémia ozbrojených síl generála Milana Rastislava Štefánika,
Demänová 393, 031 01 Liptovský Mikuláš,
E-mail: miroslav.musinka@aos.sk

GLOBÁLNA STRATÉGIA PRE ZAHRANIČNÚ A BEZPEČNOSTNÚ POLITIKU EURÓPSKEJ ÚNIE

GLOBAL STRATEGY FOR THE EUROPEAN UNION'S FOREIGN AND SECURITY POLICY

Iveta NOVOTNÁ

ABSTRACT

The current dynamic and turbulent development of human society brings many positive, but at the same time, also some negative facts are manifested in various areas of human life and the entire human civilization. In the context of the war in Ukraine, defence and security, including energy independence, became a primary topic and part of the question of the EU's place in the world and the security of its member states. This was also the case after World War II, when European countries felt the need to unite for a safer and better life, which started the integration processes that led to the creation of the EU.

Keywords: Security, Integration processes, Common foreign and security policy of the EU, Global strategy

ÚVOD

Súčasný dynamický a turbulentný vývoj ľudskej spoločnosti so sebou prináša mnohé pozitívne, ale zároveň aj negatívne skutočnosti, ktoré sa prejavujú v rôznych oblastiach života človeka i celej ľudskej civilizácie. Dôkazom toho sú početné pôvodné i novo sa objavujúce bezpečnostné hrozby a riziká, ktoré oprávnene stavajú otázky bezpečnosti na popredné miesto (Ivančík, 2021, s. 32). Bezpečnosť totiž tvorí základnú a nevyhnutnú podmienku rozvoja každej spoločnosti a dnes, v ére prehlbujúcej sa globalizácie, už neexistuje oblasť spoločenského života, ktorá by s ňou nebola spojená. Aj preto aktuálne patrí bezpečnosť k najviac frekventovaným a skloňovaným pojmom vo všetkých jeho podobách (Ivančík, 2022, s. 7).

Žiaľ, tri desiatky rokov po zásadných politických zmenách vo svete súvisiacich s koncom studenej vojny, sa Európa opäť dostáva do obdobia bezpečnostnej neistoty (Ivančík, 2019, s. 47-48). Zaistenie jej bezpečnosti, obrany, ako aj energetickej samostatnosti sa stali v súvislosti s prepuknutím konfliktu na Ukrajine primárnymi témami. Súčasná bezpečnostná situácia zásadným spôsobom aktivovala Európsku úniu (ďalej len „EÚ“) k naštartovaniu viacerých procesov, obdobne ako tomu bolo po skončení druhej svetovej vojny, resp. dvoch svetových vojen, kedy medzinárodná, ekonomická a bezpečnostná situácia v Európe aktivovala krajiny Európy k naštartovaniu integračných procesov, ktoré vyústili do vzniku EÚ.

Myšlienka zjednotenia Európy do jedného celku spolu s ideálom mierového spolunažívania medzi jednotlivými národmi a štátmi Európy sa objavovala už v antickom Grécku[1] a ovplyvňovala a formovala neskoršie moderné európske národy, vznik európskych

[1] *Achájsky spolok – skupina gréckych pobrežných miest sa spojila pod vedením stratéga Filopoiména (253 – 183 pred n. l.) za účelom ochrany a obrany pred pirátmi a mocnejšími gréckymi mestskými štátmi, ako bola aj Sparta*

štátov a ich politickú koncepciu. Európska myšlienka, alebo tzv. európsky ideál z pohľadu histórie „prešiel“ obdobím pred prvou svetovou vojnou, obdobím dvoch svetových vojen a ich medziobdobím, ktorého iniciatívy výrazne smerovali k cieľom a hodnotám európskej myšlienky – bezpečnosti a mieru na európskom kontinente, vylúčeniu vojensko-politických a ekonomických konfliktov. Snaha európskych krajín v duchu európskej myšlienky však nezabránila ďalšej vojne - druhej svetovej vojne a k zneužitiu pozitívneho obsahu európskej myšlienky fašizmom.

1 INTEGRÁCIA - HISTORICKÉ A PRÁVNE SÚVISLOSTI

Výrazný nástup realizácie európskeho ideálu sa začal až po druhej svetovej vojne (po katastrofálnych skúsenostiach a obetiach), formou integračných procesov[2], prebiehajúcich v EÚ aj v súčasnosti. Integračné procesy sa spočiatku rozvíjali v priestore západnej Európy, ktorá bola jedinou svetovou oblasťou v ktorej sa v pozadí vedecko-technickej revolúcie a za pôsobenia politických stimulov integračné procesy rozvíjali.

Cieľom integračných procesov, vychádzajúcich z Monnetovej metódy medzinárodných vzťahov[3], bolo najmä posilnenie:

vnútornej stability zainteresovaných krajín,
pozície voči socialistickému svetu,
pozície Európy voči USA,
pozície Európy vo vzťahoch s rozvojovým svetom a
potreba riešiť budúcnosť Nemecka.

Integračné európske zoskupenia v politickej oblasti sú najvyššou fázou integračných procesov - predstavujú aktivitu nielen v spoločnej hospodárskej politike, ale aj v zahraničnej, obrannej a vnútornej politike (Šíbl a kol., 2006).

Po založení Európskeho spoločenstva uhlia a oceli (ESUO), ktoré prebiehalo v období tzv. studenej vojny a vyostrenom medzinárodnom napätí (vypuknutie kórejskej vojny), prebehol v Európe neúspešný pokus o založenie Európskeho obranného spoločenstva (EOS). 27. mája 1952 podpísali zástupcovia šiestich západoeurópskych štátov, ktoré boli už členmi ESUO zmluvu o vytvorenie EOS. Francúzske Národné zhromaždenie v roku 1945 rozhodlo zmluvu neprejedať, čo znamenalo vlastne jej odmietnutie a k ratifikácii zmluvy všetkých krajín tak nedošlo (Had, Urban, 2000).

Ďalším medzníkom v zjednotení Európy bolo obdobie po páde Berlínskeho múru v roku 1989 kedy EÚ podporovala zjednotenie Nemecka a rok 1991, kedy sa rozpadlo sovietske impérium a krajiny strednej a východnej Európy za „železnou oponou“ si mohli vybrať vlastné smerovanie. Vznik nových bezpečnostných hrozieb, na ktoré nebol schopný efektívne reagovať ani jeden členský štát EÚ, bol podnetom k vytvoreniu určitých pravidiel, ktoré možno nazvať Spoločná zahraničná bezpečnostná politika (Jurčák, 2009).

Na začiatku západoeurópskeho integračného zoskupenia EÚ boli určujúcimi Parížska zmluva a Rímske zmluvy, ktoré neskôr revidoval Jednotný európsky akt, Maastrichtská zmluva, Amsterdamská zmluva a Zmluva z Nice. Maastrichtská zmluva sa stala jednotným právnym rámcom pre Európske spoločenstvá, ktorým zároveň poskytla aj politický rozmer.

– utvorili tak federálnu štruktúru, ktorá sa zachovala niekoľko storočí (European Community, č. 200, 1977, Washington, s. 29).

[2] *Integrácia – označovali sa ňou niektoré nove javy predovšetkým v medzinárodných vzťahoch, ktoré smerovali k zjednocovaniu jednotlivých krajín či skupín jednotlivých krajín v dôležitých oblastiach, najmä ekonomickej, politickej, či vojenskej, avšak toto úsilie často sprevádzali záujmové rozpory medzi štátmi, ovplyvnené aj snahou získať hegemóniu v medzinárodných integračných zoskupeniach (Šíbl, D. a kol., 2006).*

[3] *Monnetova metóda medzinárodných vzťahov kládla dôraz na uprednostňovanie práva pred silou, zjednocovanie ľudí, presun suverenity na spoločné inštitúcie, na moc inštitúcií a rovnaké práva.*

Ciele a hodnoty, ako ľudská dôstojnosť, sloboda, demokracia, rovnosť, právny štát a ľudské práva, ktoré sú súčasťou Lisabonskej zmluvy a Charty základných práv Európskej únie, tvoria základ EÚ. Všetky základné hodnoty EÚ majú spoločného menovateľa, ktorým je bezpečnosť, resp. sú závislé od bezpečnosti.

2 GLOBÁLNA STRATÉGIA AKO SÚČASŤ SPOLOČNEJ ZAHRANIČNEJ A BEZPEČNOSTNEJ POLITIKY EÚ

EÚ sa v Spoločnej zahraničnej a bezpečnostnej politike EÚ[4] (ďalej len „SZBP“) zameriava na zachovávanie mieru a posilňovanie medzinárodnej bezpečnosti, rozvoj a upevňovanie demokracie právneho štátu a zachovávanie ľudských práv a slobôd na celom svete. Cieľom SZBP, ktorej integrálnou súčasťou je Spoločná bezpečnostná a obranná politika (ďalej len „SBOP“)[5], je riešiť konflikty a podporovať medzinárodné porozumenie, prostredníctvom diplomacie a dodržiavania medzinárodných pravidiel. SZBP EÚ bola vytvorená v roku 1993 na základe Maastrichtskej zmluvy, následne posilnená nasledujúcimi zmluvami, najmä Lisabonskou zmluvou (hlava V Zmluvy o EÚ, od nadobudnutia platnosti tejto zmluvy v decembri 2009 má EÚ právnu subjektivitu, t. j. môže podpisovať medzinárodné zmluvy).

Hlavné zásady a línie SZBP určuje Európska rada, ktorá sa skladá z hláv štátov (resp. predsedov vlád všetkých členských krajín EÚ). Ústredným rozhodovacím orgánom v oblasti SZBP je Rada pre zahraničné veci, ktorá sa skladá z ministrov zahraničných vecí všetkých členských krajín EÚ a rozhodnutia prijíma v súlade s hlavnými zásadami a líniami pre oblasť spoločnej zahraničnej a bezpečnostnej politiky, stanovenými Európskou radou.

Európska komisia zohráva aktívnu úlohu pri rozvoji celkovej stratégie EÚ a navrhovaní a vykonávaní jednotlivých politík EÚ, ktoré pravidelne vyhodnocuje a predkladá o nich správy. Európska komisia spolu s ďalšími hlavnými inštitúciami EÚ tvorí celkovú stratégiu a politické smerovanie EÚ (Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ)[6].

Európska rada sa na zasadnutí v dňoch 20. - 21. júna 2019 v Bruseli dohodla na novom strategickom programe na roky 2019 – 2024, ktorý stanovuje prioritné oblasti činnosti Európskej rady a usmernení pre pracovné programy inštitúcií EÚ. Európska komisia sa v rámci priorít určených na roky 2019 – 2024 zamerala (ako na jednu zo šiestich priorít) na stratégiu silnejšej Európy vo svete (A stronger Europe in the world 2019 – 2024).

3 GLOBÁLNA STRATÉGIA EÚ A JEJ PRIORITY

Cieľom globálnej stratégie EÚ je zefektívniť reakciu EÚ na rôzne výzvy vrátane tak aktuálnej energetickej bezpečnosti, migrácie, či zmeny klímy, násilného extrémizmu a hybridných hrozieb. Celkovú stratégiu a politické smerovanie EÚ je však potrebné vnímať v širších súvislostiach.

V globálnej stratégii EÚ sa ustanovujú hlavné záujmy a zásady EÚ – je to spoločná vízia a kolektívne smerovanie EÚ. Zmluva o EÚ v jednotlivých článkoch pritom ustanovuje - zásady,

---

[4] *Ustanovenia Zmluvy o EÚ, ktoré sa týkali SZBP, boli revidované Amsterdamskou zmluvou, ktorá umožnila zefektívniť realizáciu SZBP a vytvorila funkciu Vysokého predstaviteľa SZBP (Jurčák a kol., 2009).*

[5] *Spoločná bezpečnostná a obranná politika je politika, ktorou sa stanovuje rámec EÚ v oblasti obrany a krízového riadenia vrátane spolupráce a koordinácie v oblasti obrany medzi členskými štátmi. Politika viedla k vytvoreniu vnútorných politických a vojenských štruktúr EÚ, čo umožnilo EÚ uskutočňovať vojenské a civilné misie a operácie v zahraničí. (Bližšie pozri: Ivančík – Jurčák, 2013)*

[6] *Spoločná vízia, spoločný postup: Silnejšia Európa – Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ z 28. júna 2016 a Globálna stratégia EÚ – Pohľad na uplynulé tri roky, pohľad do budúcnosti z 13. júna 2019.*

mechanizmy a postupy vykonávania spoločnej zahraničnej a bezpečnostnej politiky (Zmluva o EÚ – článok 25, článok 28, článok 29 až 31, článok 37 a článok 41).

Zásadnými dokumentami globálnej stratégie EÚ, ako súčasti SZBP, sú dokumenty „Spoločná vízia, spoločný postup: Silnejšia Európa – Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ“ z 28. júna 2016 a „Pohľad na uplynulé tri roky, pohľad do budúcnosti“ z 13. júna 2019.

„Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ“ ustanovuje päť všeobecných priorít, ktoré, ako už bolo uvedené, v októbri 2016 schválila Rada EÚ.

Ide o priority v oblasti:

- bezpečnosti a obrany,
- budovania odolnosti štátov a spoločnosti,
- integrovaného prístupu ku konfliktom a krízam,
- kooperatívneho regionálneho usporiadania,
- globálnej správy založenej na pravidlách.

Priorita **„**bezpečnosť a obrana“ - zámerom tejto priority je zlepšovať ochranu EÚ a jej občanov, pomáhať vládam pri spoločnom budovaní vojenských kapacít a rozvíjať lepšiu reakciu na krízy. Medzi opatrenia na zlepšenie bezpečnosti EÚ patrí Akčný plán v oblasti európskej obrany a Plán vykonávania v oblasti bezpečnosti a obrany.

Priorita „budovanie odolnosti štátov a spoločnosti“ - budovanie odolnosti štátov a spoločnosti prostredníctvom podpory dobrej správy vecí verejných a zodpovedných inštitúcií a prostredníctvom úzkej spolupráce s občianskou spoločnosťou, podpora sa bude zameriavať na okolité regióny EÚ na juhu a východe.

Priorita „integrovaný prístup ku konfliktom a krízam“ - integrovaný prístup ku konfliktom a krízam prostredníctvom plnej účasti vo všetkých fázach konfliktu a jednotného uplatňovania všetkých opatrení, ktoré má EÚ k dispozícii na rôznych úrovniach správy.

Priorita „kooperatívne regionálne usporiadanie“ - kooperatívne regionálne usporiadanie - bude podporovať dobrovoľné formy regionálnej správy na celom svete, ktoré štátom a národom umožnia: lepšie riadiť bezpečnostné obavy, využívať hospodárske prínosy globalizácie, plnohodnotnejšie vyjadriť svoju kultúru a identitu a uplatniť vplyv v rámci celosvetových záležitostí.

Priorita „globálna správa založená na pravidlách“ - EÚ dodržiava záväzok rešpektovať viacstranný medzinárodný poriadok založený na pravidlách a usiluje sa reformovať, pretvárať a rozširovať tento systém. EÚ plní povinnosti vyplývajúce z existujúcich iniciatív, ako sú Parížska dohoda a ciele udržateľného rozvoja, podporuje rozširovanie členstva, univerzalizáciu a plnohodnotné vykonávanie a presadzovanie povinností a iniciatív.

ZÁVER

V kontexte vyššie uvedeného je potrebné na záver zdôrazniť, že predmetná európska globálna stratégia má mimoriadny význam pre súčasnosť aj budúcnosť. Výraz „globálny“ sa pritom podľa slov bývalej vysokej predstaviteľky EÚ pre zahraničné veci a bezpečnostnú politiku a podpredsedníčky Európskej komisie F. Mogheriniovej (2016, s. 4), v rámci jej predslovu ku globálnej stratégii, nespomína len v geografickom zmysle, ale odkazuje aj na širokú škálu politík a nástrojov, ktoré sa v stratégii presadzujú. Stratégia sa zameriava na vojenské spôsobilosti a boj proti terorizmu, rovnako ako na pracovné príležitosti, inkluzívnu spoločnosť a ľudské práva.

Nanešťastie, bezpečnostná situácia a bezpečnostné prostredie sa po 24. februári 2022 zásadne zmenili a Únia musí po ruskej agresii voči Ukrajine čeliť novým výzvam – bezpečnostným, politickým, hospodárskym, energetickým a viacerým ďalším. Aj preto nielen

naši občania a naši európski spoluobčania, ale celý svet potrebujú silnú Európsku úniu ako nikdy predtým. Európsky región sa stal nestabilnejším, nepokojnejším a neistejším. Z toho dôvodu je potrebné na európskej úrovni prijímať v súlade s globálnou stratégiou efektívne a účinné opatrenia a využiť všetky relevantné a dostupné prostriedky tak na zvýšenie úrovne zaistenia vlastnej, európskej bezpečnosti, ako aj na poskytnutie pomoci Ukrajine.

Do popredia sa dostáva, okrem doposiaľ vyznávaných spoločných hodnôt EÚ a spoločnej obchodnej politiky, aj nutnosť zabezpečenia európskej obrany, potreba rozvoja a budovania vojenských spôsobilostí a kapacít, vyzbrojovania a jednoty krajín EÚ, potreba energetickej samostatnosti, ďalšieho rozširovania EÚ, potreba aktívneho konania a jednania, ako aj otázka efektívnosti fungovania medzinárodného práva, o čom svedčí aj Konferencia o budúcnosti Európy. Ruská vojenská agresia má však pre EÚ a ďalšie západné krajiny aj symbolický význam, vzhľadom na to, že predstavuje útok na základný hodnotový systém, ktorý reprezentujú (útok na hodnoty a princípy liberálnej demokracie, ľudských práv, slobody a právneho štátu, teda na jej normotvorné základy).

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

HAD, M. – URBAN, L. 2000. *Europská společenství První pilíř Europské unie*. Praha : Ministerstvo zahraničních věcí České republiky ve spolupráci s Asociácí pro studium medzinárodních vztahů v Edičním oddelení Ústavu mezinárodních vztahů, 2000. 165 s. ISBN 80-85864-88-6.

HAD, M. – PIKNA, B. 2001. *Europská společenství Druhý a třetí pilíř Europské unie*. Praha : Ministerstvo zahraničních věcí České republiky v Edičním oddelení Ústavu mezinárodních vztahů, Praha, 2001. 86 s. ISBN 80-86345-06-8.

IVANČÍK, R. 2022. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022. 240 s. ISBN 978-80-7380-873-0.

IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 32-53. ISSN 1336-9202. [online] Dostupné na: <http://ak.aos.sk/images/repozitar/vr/vr_3_2021/vr_3_2021_3.pdf>.

IVANČÍK, R. 2019. Quo Vadis európska obrana a bezpečnosť. In *Politické vedy*, 2019, roč. 22, č. 3, s. 47-67. ISSN 1335-2741. [online] Dostupné na: <http://www.politickevedy.fpvmv.umb.sk/en/archive/2019/3-2019/radoslav-ivancik.html>.

IVANČÍK, R. – JURČÁK, V. 2013. *Mierové operácie vybraných organizácií medzinárodného krízového manažmentu*. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2013. 230 s. ISBN 978-80-8040-469-7.

JURČÁK, V. a kol. 2009. *Organizácie medzinárodného krízového manažmentu.* Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2009. 235 s. ISBN 978-80-8040-387-4.

MOGHERINI, F. 2016. Foreword by Federica Mogherini High Representative of the Union for Foreign Affairs and Security Policy Vice-President of the European Commission. In *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. [online] Dostupné na: <https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf>.

PORADA, V. a kol. 2019. *Bezpečnostní vědy*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. 780 s. ISBN 978-80-758-0.

ŠÍBL, D. a kol. 2006. *Európska únia*. Bratislava : Ekonóm, Ekonomická univerzita v Bratislave, 2006. 288 s. ISBN 80 -225 - 2179-5.

ŠÍBL, D. 1998. *Medzinárodná ekonomická integrácia a Európska únia*. Bratislava : Ekonóm, Ekonomická univerzita v Bratislave, 1998. 179 s. ISBN 80 -225- 0891-8.

INTERNETOVÉ STRÁNKY

<www.epi.sk>

<www.slov-lex.sk>

<https://fmv.euba.sk/www_write/files/dokumenty/veda-vyskum/medzinarodne-vztahy/archiv/2013/3/mv_2013_3_094-105_drzka_p.pdf>

<https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=LEGISSUM:4413648>

<http://mepoforum.sk/wp-content/uploads/2016/09/EU-globalna-strategia-sk.pdf>

<https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=LEGISSUM:foreign_security_policy>

<https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0011.02/DOC_1&format=PDF>

<https://www.consilium.europa.eu/sk/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>

<https://www.eeas.europa.eu/eeas/strategic-compass-eu-0_en>

<https://ec.europa.eu/commission/presscorner/detail/sk/IP_22_924>

JUDr. Iveta NOVOTNÁ
Externý doktorand
Katedra bezpečnosti a obrany
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393, 031 01, Liptovský Mikuláš
iveta.novotna3@gmail.com

STRATEGICKÝ KOMPAS EVROPSKÉ UNIE – JEHO IMPLEMENTACE V ČESKÉ REPUBLICE

STRATEGIC COMPASS OF THE EUROPEAN UNION – ITS IMPLEMENTATION IN THE CZECH REPUBLIC

Antonín NOVOTNÝ

ABSTRACT

In the last few years, the European Union has significantly increased its ambitions in the field of security and defence. It has launched a number of programs and initiatives aimed at strengthening the Union's defence capabilities. An area where the level of coordination has so far lagged behind has been strategic planning. That has now changed. With the release of the EU Strategic Compass document on 21/03/2022, a strategic material determining the direction and goals of the European Union in the field of defence and security until 2030. The material provides a joint assessment of the strategic environment in which the EU operates and the threats and challenges the Union faces. The document contains concrete and feasible proposals with a very precise implementation schedule to improve the EU's ability to act decisively in crisis situations and defend its security and its citizens. The aim of the article is to describe the possibilities of the Czech Republic in its implementation.

Keywords: European Union, Strategic Compass, military capability, interoperability, mission and operation.

ÚVOD

„Návrat války do Evropy neodůvodněnou a nevyprovokovanou agresí Ruska vůči Ukrajině a významné geopolitické změny zpochybňují naši schopnost prosazovat naši vizi a hájit naše zájmy. Žijeme v době strategického soupeření a komplexních bezpečnostních hrozeb. Jsme svědky toho, že v našem sousedství i za jeho hranicemi přibývá konfliktů, agresí a zdrojů nestability a posiluje vojenská přítomnost, což vede k velkému lidskému utrpení a vysídlování obyvatelstva. Stále častější a z hlediska dopadu stále závažnější jsou hybridní hrozby. Vzájemná závislost je stále konfliktnější a jako zbraň je využívána měkká síla: nástroji politické soutěže jsou vakcíny, data i technologické normy. Stále více je zpochybňován přístup k volnému moři, kosmickému prostoru a digitální sféře. Čelíme rostoucímu počtu pokusů o ekonomický a energetický nátlak. Konflikty a nestabilitu navíc často vyostřuje změna klimatu, která působí jako multiplikátor hrozeb.“ (EU Strategický kompas, s.2).

EU a její členské státy čelí éře mocenské a strategické konkurence, která je umocněna vnitřními a vnějšími hrozbami ze strany autoritářských režimů. Bezpečnostní prostředí se stalo nepředvídatelnějším a nestabilnějším. To zahrnuje potřebu EU chránit své území i občany. Stejně jako sdílené hodnoty demokracie a právní stát zejména před rozsáhlými hybridními operacemi podkopávajícími demokratické procesy a obecné principy míru, mezinárodního práva a zajištění stabilního mezinárodního řádu.

Vydáním dokumentu *Strategický kompas EU – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti* dne 21.3.2022, EU

určila směr a cíle Evropské unie na poli obrany a bezpečnosti do roku 2030. Jedná se o více konkrétnější materiál, než jaký představuje Globální strategie zahraniční a bezpečnostní politiky EU, vydaná v roce 2016 (Globální strategie EU, 2016). Na přípravách Strategického kompasu se kromě relevantních národních orgánů podílela i Evropská komise, Evropská služba pro vnější činnost a Evropská obranná agentura. Byly tak vytvořeny další předpoklady pro ambicióznější EU v oblasti obrany, včetně její strategické autonomie.

V rámci německého předsednictví radě EU v červnu 2020 začal dvouletý proces tvorby tohoto dokumentu. V listopadu 2020 pak byla v rámci přípravy tohoto materiálu ve spolupráci se zpravodajskými službami všech členských zemí vypracována utajovaná analýza hrozeb, z níž dokument vychází. Konečné znění celého dokumentu a zejména hodnocení bezpečnostní situace procházelo revizí. Mezi hrozbami je mimo jiné zmiňována stále asertivnější Čína či islámský terorismus, nejvíc pozornosti však dokument věnuje Rusku, kdy ve vydané podobě již reflektuje agresi Ruské federaci vůči Ukrajině.

Mimo jiné se v dokumentu uvádí, že s návratem války na evropský kontinent a kvůli dalším nepříznivým geopolitickým posunům bude pro Evropskou unii stále obtížnější prosazovat svou vizi a bránit své zájmy. Už nebude stačit ekonomická síla – státy Unie musí zásadně navýšit svou vojenskou kapacitu, posílit odolnost proti útokům zvenčí a také zajistit daleko hlubší solidaritu a vzájemnou pomoc i součinnost, a to zejména v rámci Severoatlantické aliance (Strategický kompas EU, s.12).

Lze tak konstatovat, že Evropská unie získává dokument, který je obdobou Strategické koncepce NATO, která byla revidována a nově vydána v červnu 2022.

1 CHARAKTERISIKA A POPIS STRATEGICKÉHO KOMPASU

Přijatý dokument Strategický kompas stanovuje ambiciózní, avšak dosažitelný plán na posílení bezpečnostní a obranné politiky EU do roku 2030. Argumenty, proč EU potřebuje nový impuls v oblasti bezpečnosti a obrany, jsou jasné a přesvědčivé – agresivnější prostředí a širší geopolitické trendy vyžadují, aby EU převzala větší díl odpovědnosti za svou vlastní bezpečnost.

Strategický kompas konkrétně:

- poskytuje společné posouzení strategického prostředí EU, hrozeb a výzev, jimž EU čelí, a jejich důsledků pro EU;
- přináší větší soudržnost a společnou vizi již probíhajících činností v oblasti bezpečnosti a obrany;
- stanovuje nová opatření a prostředky s cílem:
- zajistit, aby EU mohla jednat rychleji a rozhodněji v případě krizí,
- zaručit zájmy EU a chránit občany EU posílením schopnosti EU předvídat a zmírňovat hrozby;
- stimulovat investice a inovace za účelem společného rozvoje nezbytných schopností a technologií;
- prohloubit spolupráci s partnery, zejména s OSN a NATO, v zájmu dosažení společných cílů;
- stanovuje jasné cíle a milníky pro měření dosaženého pokroku (Strategický kompas EU, s.6).

K tomu dále Strategický kompas uvádí, že ve větší míře nepřátelské bezpečnostní prostředí vyžaduje, aby EU výrazně pokročila a zlepšila své schopnosti a zvýšila ochotu jednat, posílili svoji odolnost a zajistila solidaritu a vzájemnou pomoc. Tedy vše, co je obsaženo v čl. 42 odst. 7 Smlouvy o Evropské unii (Smlouva o EU, konsolidované znění).

Jiným slovy, EU musí zvýšit svou přítomnost, efektivitu a viditelnost ve svém sousedství a na globální scéně prostřednictvím společného úsilí a investic.

Kromě úvodní části s názvem Svět, s nímž jsme konfrontováni (hodnocení bezpečnostního prostředí), je dokument je rozčleněn do čtyř oblastí (pilířů):

- Jednat (ACT)
- Zajistit bezpečnost (SECURE)
- Investovat (INVEST)
- Rozvíjet partnerství (PARTNER) (Strategický kompas EU, s.3,4).

K jednotlivým oblastem je možno dále uvést:

JEDNAT – Vždy, když vypukne krize, musí být EU schopna jednat rychle a důrazně, pokud možno společně s partnery a v případě potřeby i samostatně.

Za tímto účelem se EU zavazuje:

- posílit své civilní a vojenské mise a operace Společné bezpečnostní a obranné politiky (SBOP) tím, že jim poskytne silnější a flexibilnější mandáty, podpoří rychlé a flexibilnější rozhodovací procesy a zajistí větší finanční solidaritu a zároveň podpoří také úzkou spolupráci s ad hoc misemi a operacemi pod evropským vedením. Posílit svoji civilní SBOP prostřednictvím nového paktu, který umožní rychlejší nasazení, a to i ve složitých prostředích;
- vytvořit schopnost rychlého nasazení EU, která umožní rychle rozmístit až 5 000 vojáků v netolerantním prostředí v případě různých druhů krizí;
- posílit velitelské a řídicí struktury, zejména útvar schopnosti vojenského plánování a vedení, a zvýšit připravenost a zintenzivnit spolupráci posílením vojenské mobility a prostřednictvím pravidelných reálných cvičení v terénu, zaměřených zejména na schopnost rychlého nasazení (Strategický kompas EU, s.3).

ZAJISTIT BEZPEČNOST – Posílit schopnost EU předvídat hrozby, zaručit bezpečný přístup ke strategickým oblastem a chránit občany EU.

Za tímto účelem se EU zavazuje:

- posílit své zpravodajské schopnosti, jako je rámec společné zpravodajsko-analytické složky EU (SIAC), s cílem zlepšit informovanost o situaci a strategický výhled;
- vytvořit soubor hybridních nástrojů EU, který propojí různé nástroje umožňující odhalit širokou škálu hybridních hrozeb a reagovat na ně. V této souvislosti vytvořit specializovaný soubor nástrojů, který bude sloužit k řešení problému zahraniční manipulace s informacemi a vměšování;
- dále rozvíjet politiku kybernetické obrany EU, aby byla lépe připravena na kybernetické útoky a mohla na ně reagovat. Posílí své činnosti v námořní, vzdušné a vesmírné oblasti, zejména tím, že rozšíří koordinovanou přítomnost na moři do dalších oblastí, počínaje indicko-tichomořským regionem, a že vypracuje kosmickou strategii EU pro bezpečnost a obranu (Strategický kompas EU, s.3).

INVESTOVAT – znamená více a lépe investovat do schopností a inovativních technologií, odstranit strategické nedostatky a snížit technologickou a průmyslovou závislost.

Za tímto účelem se EU zavazuje:

- zvýšit a zkvalitnit výdaje v oblasti obrany a zlepšit rozvoj a plánování svých schopností s cílem lépe řešit operační realitu a nové hrozby a výzvy;

- hledat společná řešení s cílem rozvinout nezbytné strategické podpůrné schopnosti pro mise a operace EU, jakož i schopnosti nové generace ve všech operačních oblastech, jako jsou špičkové námořní platformy, budoucí bojové vzdušné systémy, schopnosti v kosmické oblasti a bojové tanky;
- plně využívat stálou strukturovanou spolupráci (PESCO) a Evropský obranný fond (EDF) s cílem společně rozvíjet špičkové vojenské schopnosti a investovat do technologických inovací v oblasti obrany a v rámci Evropské obranné agentury vytvořit nové centrum pro inovace v oblasti obrany (Strategický kompas EU, s.4).

ROZVÍJET PARTNERSTVÍ – v zájmu řešení společných hrozeb a výzev posílí EU spolupráci s partnery.

Za tímto účelem se zavazuje:

- posílit strategické partnerství s NATO a OSN prostřednictvím strukturovanějších politických dialogů, jakož i operační a tematické spolupráce; zintenzivní rovněž spolupráci s regionálními partnery včetně OBSE, Africké unie, a ASEAN;
- posílit spolupráci s dvoustrannými partnery, kteří sdílejí stejné hodnoty a zájmy, jako jsou Spojené státy, Norsko, Kanada, Spojené království a Japonsko; bude rozvíjet individuálně uzpůsobená partnerství na západním Balkáně, ve východním a jižním sousedství EU, v Africe, Asii a Latinské Americe;
- vytvořit fórum partnerství EU v oblasti bezpečnosti a obrany s cílem zajistit užší a účinnější spolupráci s partnery při řešení společných výzev (Strategický kompas EU, s.4).

2 IMPLEMENTACE STRATEGICKÉHO KOMPASU V PODMÍNKÁCH ČESKÉ REPUBLIKY

Od července letošního roku je ČR předsednickou zemí Rady EU. Česká republika se během svého předsednictví zaměřuje na pět úzce provázaných prioritních oblastí:

- Zvládnutí uprchlické krize a poválečná obnova Ukrajiny
- Energetická bezpečnost
- Posílení evropských obranných kapacit a bezpečnost kybernetického prostoru
- Strategická odolnost evropské ekonomiky
- Odolnost demokratických institucí (České předsednictví v radě EU, on line).

Jednou z těchto prioritních oblastí je tedy i oblast bezpečnostní a obranné politiky, v rámci, které se české předsednictví zaměřuje na posílení společných evropských obranných schopností a bezpečnosti kyberprostoru. Role a cíle českého předsednictví v oblasti bezpečnosti a obrany spočívají v implementaci vybraných postupů a nástrojů Kompasu do praxe. V oblasti budování odolnosti EU se české předsednictví zaměřuje především na rozvoj a realizaci tzv. „toolboxových iniciativ“. Jedná se zejména o EU Hybrid Toolbox, jehož cílem je shrnout dosavadní metody boje proti hybridním hrozbám do soudržné koncepce, včetně preventivních, kooperativních nebo omezujících opatření posilujících vzájemnou solidaritu a pomoc mezi členskými státy (Strategický kompas EU, s.3). Předsednictví České republiky tak pracuje především na vytvoření a zprovoznění tohoto souboru nástrojů tak, aby byla zajištěna jednotná reakce členských států na hrozby hybridní povahy (České předsednictví v radě EU, on line).

V průběhu francouzského předsednictví v první polovině roku 2022, se členské státy dohodly na definici hybridních hrozeb a přijetí Rámce pro koordinovanou reakci na hybridní hrozby a kampaně. Bylo rovněž doporučeno předložit návrh na zřízení tzv. týmů rychlé

reakce pro oblast hybridního působení (EU Hybrid Rapid Response Teams) a předložit obnovenou verzi Operačního protokolu pro boj proti hybridním hrozbám (EU Playbook) (EC consultation: the new Cyber Resilience Act). V rámci českého předsednictví by měly být obě iniciativy do konce roku 2022 předloženy Radě, jejíž orgány na návrzích průběžně pracují.

V rámci oblasti odolnosti se dále ČR zabývá také dezinformacemi a strategickou komunikací na úrovni EU. Odhalování, analýza a včasná reakce na dezinformační kampaně jsou součástí souboru nástrojů proti manipulaci s informacemi a zahraničním vměšováním (tzv. FIMI Toolbox). V červenci 2022 byly schváleny Závěry Rady, které zdůraznily potřebu nepřetržité práce na vývoji FIMI Toolboxu a potřebu využití všech dostupných prostředků ke zvýšení povědomí o současném stavu strategického prostředí, v němž EU působí. ČR také dále pokračuje v rozvoji politik EU v oblasti kybernetické obrany a souboru diplomatických nástrojů pro reakci na působení v oblasti kybernetického prostoru (EU Cyber Diplomacy Toolbox). Poskytne tak platformu pro diskusi o návrhu, jak chránit orgány, instituce a jiné subjekty EU před kybernetickými útoky, kde se očekává prosazení obecného přístupu Rady. Pozornost je také věnována Nařízení o kybernetické odolnosti (Cyber Resilience Act) (Strategický kompas EU, s.23).

Pokud by se českému předsednictví podařilo tyto zásady prosadit, přispělo by to k prosazování jednotných bezpečnostních požadavků pro společnosti vyvíjejícími a obchodujícími s digitálními technologiemi. Tyto společnosti totiž často nezavádějí dostatečné bezpečnostní postupy na ochranu jednotlivých komponentů, výrobků a dodavatelských řetězců před možnými kybernetickými útoky (EC consultation: the new Cyber Resilience Act).

Kromě jednotlivých nařízení a pravidel klade české předsednictví důraz na implementaci Strategie kybernetické bezpečnosti EU (EU Cybersecurity Strategy) (Strategický kompas EU, s.28) a také usiluje o pokrok ve vývoji Vesmírné strategie EU pro bezpečnost a obranu (EU Space Strategy for Security and Defence). Do konce roku 2022, na základě harmonogramu uvedeného ve Strategickém kompasu, by Galileo a jeho mechanismus odolnosti vůči hrozbám (Threat Resilience Mechanism), měly projít základním validačním procesem (Strategický kompas EU, s.28).

Ve stejném časovém rámci by jednotlivé členské státy EU ve spolupráci s Evropskou agenturou pro kosmický program (EUSPA) měly prozkoumat možnosti prohloubení spolupráce, vzájemné solidarity a pomoci v případě ohrožujících aktivit přicházejících z kosmického prostoru. V oblasti kosmického programu EU má ČR jako hlavní prioritu vytvoření programu EU pro bezpečnou konektivitu, který však není součástí Kompasu jako takového (České předsednictví v radě EU, on line). Soubor nástrojů EU pro boj proti hybridním hrozbám je klíčem k budování odolnosti vůči hybridním útokům, zejména k ochraně kritické infrastruktury, kybernetické bezpečnosti a boji proti dezinformacím.

Kompas dále označuje oblasti, které potřebují rozvoj spolupráce se spojenci, jako je NATO, aby si mohly vyměňovat informace o sdílených hrozbách a budovat tak efektivnější včasné systémy reakce. Užší koordinace mezi EU a NATO je důležitá nejen proto, aby se zabránilo zdvojování civilního a vojenského využívání těchto technologií, ale také pro koordinaci investic, směrování zdrojů a optimální využití rozvoje kapacit dvojího užití armádou (The V4 towards a new NATO Strategic Concept and the EU Strategic Compass).

České předsednictví, v souladu se Strategickým kompasem, pracuje na překonání nedostatků v oblasti obranných investic. Je zásadní účinněji spravovat výdaje v rámci Evropského obranného fondu a zároveň vhodně aplikovat nově vznikající nástroj, tzv. Evropský program obranných investic (EDIDP, on line), který by měl fungovat jako platforma pro vzájemnou spolupráci v oblasti obstarávaní bezpečnostních a obranných kapacit pro členské státy Unie (Defence Investment Gaps Analysis). Návrh na zavedení tohoto

mechanismu je také předmětem vyjednávání v Radě v průběhu českého předsednictví. (České předsednictví v radě EU, on line).

Při implementaci Kompasu se předsednictví také zaměřuje na iniciativy ve společném obranném výzkumu a vývoji na podporu inovativní a konkurenceschopné obranné struktury EU. V oblasti rozvoje společných obranných schopností dále usiluje zejména o posílení obranných schopností EU, schopnosti reagovat v krizových situacích a na implementaci nařízení o zřízení sil rychlé reakce a zefektivnění misí SBOP (České předsednictví v radě EU, on line).

V oblasti posilování evropských obranných kapacit se ČR také snaží rozvinout koordinovanější spolupráci s NATO tak, aby nedocházelo k duplikaci procesů. K tomu patří i identifikace příležitosti k mezinárodní spolupráci (CARD, on line) a jejich realizaci prostřednictvím programů jako Stálá strukturovaná spolupráce (PESCO, on line) nebo kapacit Evropského obranného fondu (EDF, on line).

ZÁVĚR

Vývoj i přijetí dokumentu Strategický kompas EU je novou kapitolou evropské integrace, které otvírá nové možnosti společné spolupráce členských zemí EU v oblasti bezpečnosti. K tomu může přispět i Evropský obranný fond, protože jeho logikou bylo nejdříve společně vyvíjet, později také ulehčovat nákup a v konečném důsledku i vojensku spolupráci.

Jedním z plánů je, že EU by měla společně identifikovat nedostatky, které v obraně jsou, a snížit svou závislost na nákupu vojenských technologií ze států mimo EU. Součástí je i analýza slabých míst evropské obrany, z níž by společné projekty a nákupy techniky měly vycházet. Bez investicí do evropských produktů, ať už společných nebo co nabízí jednotlivé evropské země, se EU k autonomii těžko přiblíží.

Strategický kompas tak počítá s budoucím financováním evropské obrany ze společného rozpočtu a zejména s podstatným navýšením národních vojenských rozpočtů. Česká republika se přihlásila k závazku dosažení 2 % HDP do roku 2024, které budou prioritně určeny na nové obranné akvizice – stíhací letouny, tanky nebo bojová vozidla pěchoty.

Dokument prosazuje intenzivnější spolupráci mezi evropskými zbrojními podniky, prověřování komplementarity vybavení evropských armád nebo společných nákupů zbraní evropského původu. Součástí je i diskuse, že takové nákupy by mohly být osvobozeny od daně z přidané hodnoty a také že by si EU mohla na světových trzích půjčit další peníze určené na posílení evropské obranyschopnosti.

Nejviditelnějším projevem nové evropské obranné politiky je jednotka rychlého nasazení o pět tisících vojácích složená z prvků pozemních, leteckých i námořních sil, společně vycvičených a schopných se pružně přizpůsobit potřebám i konkrétním situacím.

Doposud všechny snahy vytvořit nějaké evropské jednotky skončily nezdarem. V tomto případě se zdá, že EU a její Strategický kompas, který vypadá jako skutečně komplexní a ucelený základ budoucí obranné politiky, pro to vytváří daleko reálnější předpoklady. Lze tedy doufat, že v roce 2025, kdy tento dokument předpokládá revizi, už bude tento cíl do určité míry dosažen.

SEZNAM BIBLIOGRAFICKÝCH ODKAZŮ

CARD. (on line). [cit. 2022-09-20]. Dostupné na internetu: https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)

COUNCIL OF THE EU, ed. SMLOUVA O EVROPSKÉ UNII (KONSOLIDOVANÉ ZNĚNÍ), EUR-Lex, Access to European Union law, Brussels, Belgium, 2012. [cit. 2022-09-20]. Dostupné na internetu: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0008.02/DOC_1&format=PDF

COUNCIL OF THE EU, ed. COUNCIL DECISION establishing the list of projects to be developed under PESCO, EUR-Lex, Access to European Union law Brussels, Belgium, 2018. [cit. 2022-09-20]. Dostupné na internetu: http://data.consilium.europa.eu/doc/document/ST-6393-2018-INIT/en/pdf

COUNCIL OF THE EU. (2022). Council conclusions on a Framework for a coordinated EU response to hybrid campaigns. [cit. 2022-09-20]. Dostupné na internetu: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

České předsednictví v radě EU (on line). [cit. 2022-09-20]. Dostupné na internetu: https://czech-presidency.consilium.europa.eu/cs/program/priority/

EDA. Capability Development Plan. Brussels, Belgium 2018. [cit. 2022-09-20]. Dostupné na internetu: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f

EDF. (on line) [cit. 2022-09-20]. Dostupné na internetu: https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/european-defence-fund_en

EDIDP. (on line). [cit. 2022-09-20]. Dostupné na internetu: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en

EU. Sdílená vize, společný postup: silnější Evropa, Globální strategie zahraniční a bezpečnostní politiky Evropské unie. Brusel, June 2016. 37 s. [cit. 2022-09-20]. Dostupné na internetu: https://mocr.army.cz/assets/dokumenty-a-legislativa/eu/eugs_cz_version.pdf

EU. *Strategický kompas EU – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti.* [cit. 2022-09-20]. Dostupné na internetu: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/cs/pdf

EUROPEAN COMMISSION. (2022). Defence Investment Gaps Analysis. [cit. 2022-09-20]. Dostupné na internetu: https://ec.europa.eu/info/publications/defence-investment-gaps-and-measures-address-them_en

PESCO. (on line). [cit. 2022-09-20]. Dostupné na internetu: https://www.pesco.europa.eu/

Senior Defence Experts. (2021). The V4 towards a new NATO Strategic Concept and the EU Strategic Compass. [cit. 2022-09-20]. Dostupné na internetu: https://www.europeum.org/data/articles/the-v4-towards-a-new-nato-strategic-concept.pdf

Simmons + simmons. (2022). European Commission consultation: the new Cyber Resilience Act. [cit. 2022-09-20]. Dostupné na internetu: https://www.simmons-simmons.com/en/publications/cl1c5j6y41bue0a316peubejz/european-commission_consultation-the-new-cyber-resilience-act

Ing. Antonín NOVOTNÝ, Ph.D.
Centrum bezpečnostních a vojenskostrategických studií
Univerzita obrany
Kounicova 65
662 10 Brno
E-mail: antonin.novotny@unob.cz

VYTVÁŘENÍ NOVÉ MOCENSKÉ AUTORITY V SYSTÉMU MEZINÁRODNÍCH VZTAHŮ. OD VIZE K REALITĚ

CREATING A NEW POWER AUTHORITY IN THE SYSTEM OF INTERNATIONAL RELATIONS. FROM VISION TO REALITY

Jindřich NOVÝ

ABSTRACT

The paper deals with the issue of the origin and structure of power authority as a part of the system of international relations. It describes the individual pillars of the formation and functioning of such an entity. Using the example of emerging-market countries, he points to the fact that, in addition to traditional centers of power, other new structures with such ambition are emerging. And it is imperative to take such activities very seriously, as they can play an important role in the future. Particular emphasis is placed on expanding the number of countries that are involved in the activities of emerging economies and thus support their international authority.

Keywords: Power authority, BRICS, New Developmnet Bank, Shangai Cooperation Organisation, pillars of international authority

ÚVOD

Pokud se blíže zaměříme na studium v oblasti mezinárodních vztahů a reálných mezinárodních systémů v interakci jednotlivých států a skupin států v jejich konkrétní historické podobě, potom se často zabýváme otázkou jejich struktury a vzájemných vztahů. V dostupné odborné literatuře se často klasifikace, popisy a konkrétní podávaná podoba těchto vztahů mnohdy liší, a to často podle úhlu pohledu autora takového pojednání.

V celkovém systému uspořádání mezinárodních vztahů, především po druhé světové válce, je patrná určitá a zjevná polarita, která se v jejich různosti projevuje. Různé země a skupiny zemí nadále usilují o získání mocenských pozicí, které by jim lépe umožnily realizaci jejich cílů. V průběhu doby se měnili aktéři a měnila a mění se také struktura a intenzita vlivu těchto mocenských center na politický, ekonomický a bezpečnostní vývoj ve světě.

Struktura, vztahy mezi reálnými mocenskými autoritami se postupně utvářely od podoby poválečné bipolarity (dominance USA a SSSR) až po poměrně složitou interakci současné podoby globální multipolarity.

Multipolarita v uspořádání mezinárodních vztahů není vůbec novým konceptem, ale prosazuje se v měnících se podmínkách. V posledních letech jsme svědky, že se na základě vývoje mezinárodních vztahů postupně formuje a rozšiřuje nová struktura mocenské autority a to především v oblasti tzv. rozvíjejících se ekonomik.

V samotném příspěvku je věnována pozornost vývoji v tzv. Euroasijské oblasti, což je spíše pojem geopolitický, než ryze zeměpisný. V současném vývoji se však dění v této části světa věnuje poměrně značná pozornost především proto, že se zde odehrávají potenciálně zajímavé události, které mohou do značné míry později ovlivnit chod světa.

Smyslem tohoto příspěvku je, aby poukázal na proces vzniku nové mocenské autority, která stále zřetelněji vstupuje do systému mezinárodních vztahů. Poukázat na obsah a strukturu

pilířů (platforem), na kterých tato nově se rodící mocenská autorita již teď stojí. V neposlední řadě autor směřuje pozornost na skutečnost, jakou roli a význam může takové mocenské uskupení, resp. mocenská autorita mít v budoucnu vzhledem ke svému lidskému, ekonomickému a vojenskému potenciálu.

Účelem ani ambicí příspěvku není jakkoli politické postoje obhajovat nebo dehonestovat. Skutečností zůstává, že na reálný vývoj situace mají aktéři často velmi protichůdné názory. Spíše poukázat na způsob myšlení a argumentaci zúčastněných zemí.

1 MEZINÁODNÍ VZTAHY A KONCEPT MULTIPOLARITY

Podle Krejčího (Krejčí,1997) je mezinárodní systém tradičně *určován charakterem aktérů mezinárodních vztahů, vztahy mezi těmito aktéry a normami, resp. regulátory jejich chování.* (Krejčí, 1997). Jedná se právě o to, jaký charakter, jaké vztahy, jaké normy tyto aktéři realizují a jakým chováním se vyznačují. Analýza reálného mezinárodního systému je kontinuálním procesem, protože se situace v této oblasti neustále vyvíjí.

Bývalý ministr zahraničních věcí Lubomír Zaorálek vyjádřil novost současné situace za pomoci citace z poslední národní bezpečnostní strategie USA, když uvádí: „*V poslední národní bezpečnostní strategii USA se praví, že stojíme na prahu nového času: Míříme do éry trvalého soupeření velkých mocností, na které Západ není připraven.“ Všichni cítíme, že řád světa, tak jak jsme ho dříve znali, nefunguje, a stěží se lze vrátit zpět. Nová pravidla tu ale ještě nejsou a my žijeme v nejistotě a strachu z bouře, která může přijít.“* (Zaorálek, 2019). Z tohoto hlediska se jeví jako užitečné, abychom se blíže zabývali relativně novými jevy a skutečnostmi, ke kterým dochází v systému uspořádání mezinárodních vztahů.

V rámci existujících reálných mezinárodních systémů existují snahy jejich aktérů po získání dominance v jejich rámci, aby tak mohli lépe uskutečňovat své vlastní zájmy. Tato tendence doprovází vývoj mezinárodních vztahů v celých moderních dějinách a setkáváme se tak s pojmy, jako jsou polarita. Podle Harta „*polarita vyjadřuje počet autonomních center moci a je funkcí rozdělení moci pouze mezi nejvýznamnější aktéry.“* (Hart, 1985, s.31).

V současné době nejčastěji hovoříme o tom, že mezinárodní vztahy, co se týče polarity vztahů prošly obdobím bipolarity po druhé světové válce, kdy se profilovaly jednoznačně mocnosti USA a Svaz sovětských socialistických republik. Postupně se na světové scéně začaly profilovat další země nebo integrovaná uskupení. Bylo to např. Japonsko nebo tzv. „nově industrializovaná centra“ a státy integrující se Evropy. Zásadní strategická rozhodnutí už nebylo možné uskutečnit minimálně bez konzultace s těmito subjekty. Výrazné změny je možné sledovat od počátku 21. století. Tyto změny jsou charakteristické mimo jiné komplexním vlivem globalizace a způsoby, jak na novou situaci reagovaly státy a jejich koalice. Jejich vzájemné působení vytváří situaci, kterou teorie mezinárodních vztahů definuje jako multipolaritu v uspořádání mezinárodního systému.

Tuto definuje např. Waisová následovně *„Multipolarita popisuje stav rozptýlení či rozdělení moci v systému mezi více než dva aktéry. Multipolarita může mít různý charakter – může mít charakter omezené multipolarity, kdy je v systému přítomno jen několik velmocí, může mít však i charakter extrémní multipolarity, kdy je moc rozptýlená mezi velké množství hráčů. Multipolární systém je mnohem náchylnější ke konfliktům, než systém unipolární nebo bipolární. Celý systém je méně předvídatelný než systémy předchozí“* (Waisová,2009, s. 51).

2 MOCENSKÁ AUTORITA A JEJÍ PILÍŘE

Autor používá v příspěvku pojem **mocenská autorita**. Jedná se o poměrně vnitřně složitou kategorii, která je často zkoumána především v sociologii a také filozofii.

Koncepcí moci se zabývala a zabývá řada předních světových i tuzemských učenců. Podle známé knihy Antonyho Giddense Sociologie můžeme moc definovat jako *„schopnost jedinců nebo skupin prosadit své vlastní zájmy nebo záměry i přes odpor druhých“* (Giddens, 1999). Moc se uplatňuje ve všech společenských vztazích (například kolektiv vs. jednotlivec). Je to také schopnost prosadit svou vůli. Moc může náležet jednotlivci, skupině lidí, státu, můžeme o ni hovořit i v obecnějším pojetí.

Teorií moci a autority se zabýval mimo jiných přední sociolog Max Weber. Jak uvádí ve své publikaci Jandourek (Jandourek, 2003) *„Autorita je podle něho uznávána na základě nároku, kompetence a převahy. Weber dělí autoritu na osobní, primární a abstraktní.“*

V mezinárodních vztazích státy a skupiny států usilují o získání mocenské autority jako způsobu k prosazování vlastních politických, ekonomických a vojenských zájmů, které jsou státům usilujícím o tuto pozici společné a na kterých nacházejí společnou shodu.

Tento proces autor zkoumá v podmínkách skupiny zemí tzv. rozvíjejících se ekonomik, později obecně nazývaných akronymem BRICS[1], tedy uskupení zemí, které začaly významněji hovořit do systému mezinárodních vztahů v první dekádě nového tisíciletí. Dále příspěvek popisuje, jakou roli a úlohu hraje toto uskupení v roli nově vytvářené mocenské autority.

Robert Keohane na tuto otázku odpovídá tak, že *instituce se etablují buď proto, že je velmoci vytvářejí, aby snížily transakční náklady, zavedly normy a pravidla ve svůj prospěch nebo reagovaly na poptávku po nich. Tento vývoj se zpravidla odehrává v hlavních stycích mezinárodních dějin, kde nejisté prostředí buď volá po velmocenských intervencích, nebo klade silné požadavky na vytvoření institucí zajišťujících stabilitu* (Koehane, 1984).

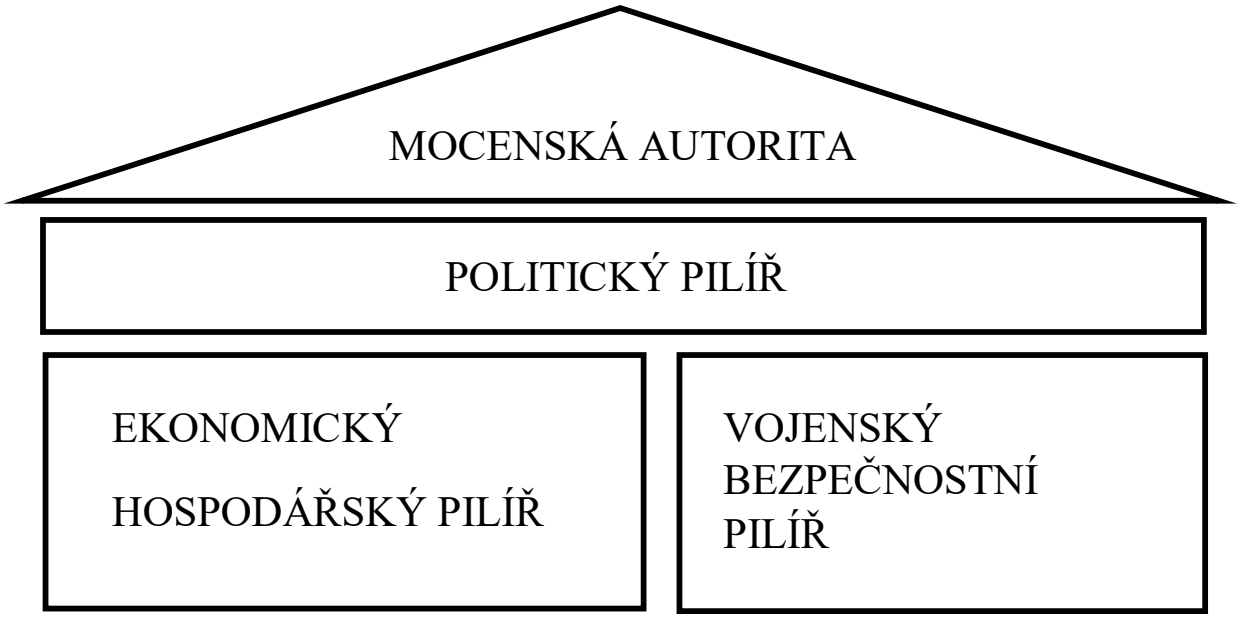
Proces vzniku takových mocenských autorit v podobě institucí má různou dynamiku i různý průběh. Každá fungující mocenská autorita v současnosti je odlišná v mnoha prvcích. Některé autority vznikají s dobře navrženými strukturami a pečlivě vytvořenými dlouhodobými cíli. Za takové instituce lze považovat Brettonwood Systém a OSN. *Jindy se státy (některé se ujímají vedení) sejdou, aby vytvořily instituce, které se zabývají konkrétními problémy a později rozšiřují své mandáty, posilují své struktury a přidělují jim další úkoly.* (Fredholm, 2012).

Pro postupný vznik a formování nové mocenské autority bylo a je typickým jevem, že účastnické země projevují a deklarují dlouhodobou nespokojenost s reálným uspořádáním mezinárodních vztahů ve světě, mají pocit, že jejich emancipační snahy nejsou dostatečně reflektovány. A proto motivem k vytváření takové struktury je snaha změnit své mocenské postavení vůči již existujícím mocenským autoritám. Potvrzuje to např. i Acharya, když píše, že *vznikající mocnosti nejsou však spokojeni ani s mocenskou strukturou, pravidly a postupy* , které i přes měnící se rozdělení moci i nadále upřednostňují zavedené velmoci (Acharya, 2018).

Co se týče nově vznikající mocenské autority, je možné konstatovat, že se nejedná o nějak vnitřně přísně uspořádanou skupinu zemí a jasně deklarovanými konkrétními společnými hodnotami a zájmy, ale spíše skupinou, která zatím diskutuje v krátkodobém horizontu společné postupy. Vůči ostatním zemím vystupují ovšem relativně jednotně. To ale nevylučuje, že v některých aspektech se tyto státy nemohou odlišovat. Jistá míra odlišnosti je vlastní každé koalici, která usiluje o moc v širším kontextu. Pokud hovoříme o aspektech rodící se nové (rozuměj, dosud reálně neexistující) mocenské autority v mezinárodních vztazích, bylo by dobré si ujasnit, na jakých pilířích, resp. Platformách taková mocenská autorita stojí a co vytváří její váhu v systému mezinárodních vztahů.

Tyto základní pilíře autor znázornil za pomoci známého obrázku “antického chrámu.“ Na jakých pilířích tedy stojí např. nově se formující mocenská autorita?

[1] Výraz BRIC použil poprvé analytik investiční skupiny Goldman and Sachs Jim O´Neill. In. Global Economics Paper No. 66. *Building Better Global Economic BRIC. 30. November 2001.* Dostupné na: http://www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-bric.pdf lze považovat



Obrázek 1 Základní pilíře mocenské autority
Zdroj: autor

Aby mohla mocenská autorita vůbec vzniknout, fungovat a ovlivňovat dění ve svém okolí, musí postupně vytvářet, upevňovat a budovat minimálně **tři základní pilíře**, na kterých bude reálně existovat.
Těmi to pilíři jsou:

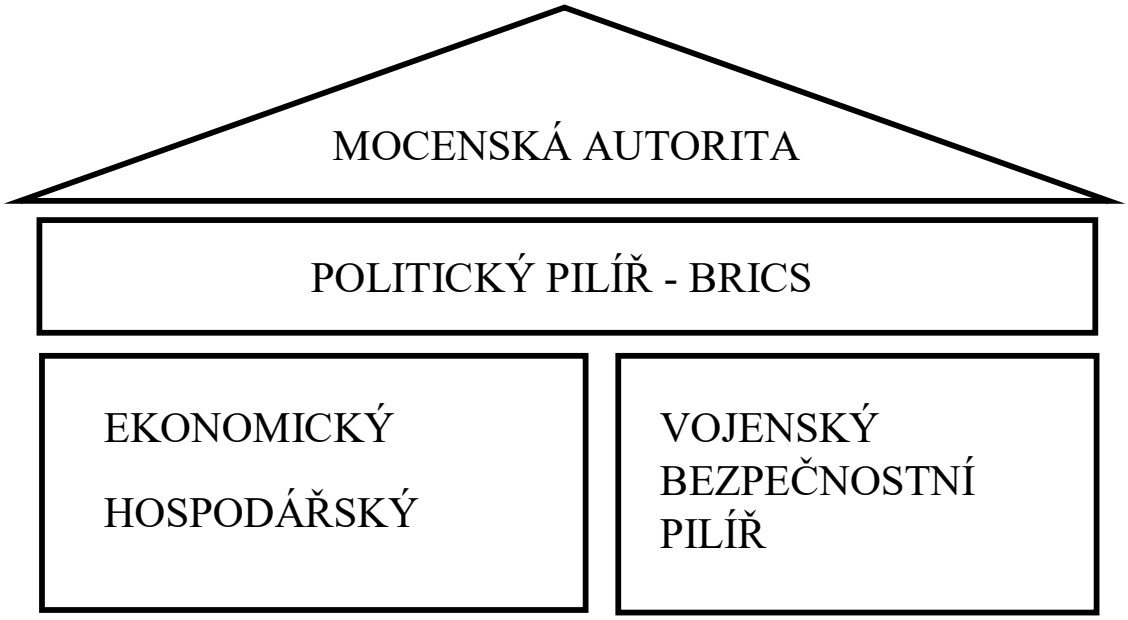
- **Politický pilíř**, jako sjednocující systém konkrétních vzájemných vztahů a hodnot, na půdorysu kterých se jednotliví účastníci sdružují. Představuje deklarované hodnoty a obecné cíle, které sleduje a které jsou podporovány dalšími pilíři, které jsou nezbytné pro realizaci konkrétní síly.
- Pro reálnou existenci mocenské struktury jsou nezbytné, vedle politických, také reálné **ekonomické a hospodářské zdroje**, kterými může reálně disponovat. V konkrétní době a v konkrétním prostředí se jedná o soubor ekonomických norem, pravidel, ale také nástrojů, kterými prosazuje své ekonomické zájmy a priority.
- **Vojenský a bezpečnostní pilíř** ve svém souhrnu zahrnuje reálné aspekty a možnosti ochrany a obrany společně deklarovaných zájmů. V interakci se světovým okolím se musí být schopná taková autorita prosadit a obhájit své postavení reálnými vojenskými a bezpečnostními strukturami.

Těmto často turbulentním událostem určuje směr a obsah pohybu především uskupení zemí rozvíjejících se ekonomik, známých pod zkratkou BRICS. V průběhu posledních zhruba deseti let se mezi těmito zeměmi odehrává mnoho událostí, které nepostačuje jen registrovat, ale ukazuje se jako užitečné je analyzovat především z hlediska vytváření potenciálu, který má stále větší schopnost ovlivňovat reálné dění nejen v oblasti Euroasie.

Do tohoto prostoru se soustředí síla, která může v následujícím období (pokud tomu již není v této době) být jedním z hlavních center světového vývoje. Situace se ale pod vlivem reálné politické a vojenské situace vyvíjí a mění. Především z hlediska vytváření a formování potenciálu, který má schopnost později výrazně ovlivňovat chod světového dění. V některých oblastech společenského života a v některých zeměpisných oblastech už k tomu dochází.

Proto se v dalším příspěvek věnuje tomu, zda, jak a čím státy skupiny BRICS naplňují požadavky na vytvoření mocenské autority v jednotlivých pilířích. Také je nezbytné sledovat tu skutečnost, že se platforma zemí, uskutečňujících aktivity v jednotlivých pilířích stále rozšiřuje a získává větší mezinárodní vliv.

3 BRICS JAKO POLITICKÝ PILÍŘ



Obrázek 2 BRICS jako politický pilíř mocenské autority
Zdroj: autor

Když v roce 2001 poprvé analytik investiční společnosti Goldman and Sachs Jim O´Neill použil akronym BRIC (tehdy ještě bez Jihoafrické republiky), mohl jen málokdo tušit, že se z poměrně zajímavé myšlenky může postupně stávat ještě zajímavější realita.

Základem pro společnou činnost zkoumaných států v oblasti se stal vznik, existence a rozvoj společenského uskupení států, pro které se ujal akronym BRICS, který představuje v užitém schématu mocenské autority tzv. „politický pilíř" její existence.

BRICS je charakterizována jako neformální skupina států zahrnující Brazilskou federativní republiku, Ruskou federaci, Indickou republiku, Čínskou lidovou republiku a Jihoafrickou republiku. Byla to ruská strana, která iniciovala vytvoření BRICS. Dne 20. září 2006 se na návrh ruského prezidenta Vladimira Putina na okraj zasedání Valného shromáždění OSN v New Yorku konalo první ministerské zasedání BRICS. Setkání se zúčastnili ministři zahraničních věcí Ruska, Brazílie a Číny a indický ministr obrany. Vyjádřili zájem o rozšíření mnohostranné spolupráce. Uskupení BRICS dnes spojuje státy s rozdílnými politickými systémy a je zřejmé, že ani jejich politická, ekonomická a vojenská trajektorie není v každém ohledu jednotná.

K jeho existenci v počátcích jeho působení vládl, a nutno říct, že i dnes vládne vlastně u mnoha autorů skepse a pesimismus. Tyto postoje pramení spíše z toho, že svou činností nenaplňuje zvyklostní definici politické koalice. Na toto téma profesorka Börsel napsala, že *„…být globální mocností vyžaduje více než ekonomické zdroje. BRICS musí rozvinout vizi globálního řádu a mít politickou vůli využít svých schopností k jeho prosazování. Zatím se zdá,*

že jejich chuť ke globálnímu vůdcovství je omezená. Spíše se zabývají utvářením řádu regionu, ve kterém jsou zakotveni" (Börsel, 2012).

Toto, na první pohled nesourodé společenství států se postupně (a přes mnohé překážky) průběžně formuje do podoby platformy, na které zúčastněné země realizují politické dohody, ujednání, které se dále promítají do dalších oblastí, jako je ekonomika a vojenská struktura. Je ve struktuře zkoumané mocenské autority prioritním pilířem.

Skutečnost že tyto země nekopírují, evropskou, euroatlantickou tzv. „západní" představu týkající se uspořádání mezinárodních vztahů, o vzniku a fungování politických koalic a uskupení, ještě neznamená, že jejich představy a způsob realizace vztahů v mnoha oblastech vylučuje jejich společný postup a vnitřní akceschopnost takového uskupení. Z původně nesouvislé skupiny, vlastně „vynalezené" ekonomy a novináři, se BRICS postupně mění v úžeji spjatý blok, který svůj hospodářský potenciál chce využít i geopoliticky.

Státy skupiny BRICS hrají podle všech dostupných údajů zásadní roli ve světové ekonomice. V reálných údajích je patrné, že vliv těchto zemí nadále poroste a ony jsou si své emancipace na světovém hospodářství vědomy. Dlouhodobě je sjednocuje pocit, že jsou západem a USA přehlíženými a nedoceňovanými partnery, a proto se snaží dlouhodobě budovat alternativní ekonomický systém s nízkou závislostí na „Západu."

Na otázku, co sbližuje národní státy v této skupině, odpověděl bývalý náměstek generálního tajemníka OSN a indický ministr zahraničních věcí Shashi Tharoor *„Jak už to bývá, jedním z atributů, které všichni členové BRICS sdílejí, je jejich vyloučení z míst, o kterých se domnívají, že si je v současném světovém řádu zaslouží. A upírání legitimních pozic na globální scéně dnešními dominantními mocnostmi se ukazuje jako velmi silné lepidlo, které drží seskupení pohromadě. BRICS se pomalu vynořují jako alternativní fórum, které se dokáže postavit dominantnímu světonázoru zavedených ekonomik. Na zemích BRICS možná v roce 1945 nezáleželo, ale tohle je rok 2022 – ignorovat BRICS znamená ignorovat přelom dějin"* (Tharoor, 2016).

Od svého založení se členové BRICS setkávají na výročních summitech, kterých zatím proběhlo 14, aby diskutovali o otázkách z různých oblastí společenského života členských zemí. První oficiální summit se konal v Jekatěrinburgu v červnu roku 2009. Od té doby se čelní představitelé členských zemí scházejí pravidelně a výstupy z jednání zveřejňují v podobě uceleného dokumentu, který je veřejně přístupný. Každý z níže uvedených summitů má nějaké konkrétní zásadní téma, ke kterému se přijímají společné závěry. Zvláštností v činnosti tohoto uskupení je dobrovolnost plnění těchto závěrů a absence přísně organizovaného byrokratického aparátu určeného k jejich kontrole a vymáhání, jak jsme zvyklí například z činnosti Evropské unie.

3.1 ROZŠIŘOVÁNÍ BRICS

Současná struktura a pozice uskupení BRICS není konečná, ani definitivní. Členské země reagují na aktuální vývoj ve světě a nejen, že počítají s rozšířením, ale v tomto směru již realizují konkrétní kroky. Na posledním setkání hlav států v Pekingu byla projednávána možnost rozšíření skupiny a přidání nových členů, jmenovitě Íránu, Saúdské Arábie a Argentíny.

V procesu rozšiřování členských států BRICS byl učiněn první důležitý krok. Mluvčí íránského ministerstva zahraničí oznámil 27. června 2020 podání žádosti Íránu o vstup do BRICS. Zároveň , podle agentury Reuters, prezident Íránu Ebrahim Raisi vyjádřil ochotu

Teheránu podělit se o své rozsáhlé schopnosti, aby pomohl BRICS dosáhnout jejich cílů.[2] Podobný krok připravuje v nejbližší době podle vyjádření jejích představitelů také Argentína. Jak uvádí Pavcic, prezidentka BRICS Purmina Anand oznámila *„že Saúdská Arábie, Turecko a Egypt zahájily proces provedení stejného kroku* (Pavcic, 2022).

Koncepce BRICS+, kterou široce diskutoval a prezentoval na Světovém ekonomickém fóru v roce 2018 Jurij Lisovolik[3] programový ředitel Valdajského diskusního klubu představil relativně nový strategický koncept rozšiřování působnosti uskupení, který by v současné podobě zahrnoval asi 35 zemí. To by vedlo k zahájení éry tzv. „vertikální globalizace." Iniciativa BRICS+ tedy spíše než o prosté rozšíření základního sektoru členů, usiluje o vytvoření nové platformy pro vytváření regionálních a bilaterálních aliancí napříč kontinenty a zaměřuje se na spojení regionálních integračních bloků, v nichž ekonomiky BRICS hrají vedoucí roli.

18. dubna 2018 Jim O´Neill, bývalý předseda Goldman Sachs Asset Management a bývalý britský ministr financí uvedl, že „*Zatímco Čína a Indie nadále pohánějí globální ekonomiku, připojuje se k nim řada dalších zemí s vysokým počtem obyvatel a vysokým potenciálem, zejména v Asii. Je stále jasnější, že budoucí růst nebude založen pouze na jedné mocné zemi, ale na celoregionálních přírůstcích prosperity* (O´Neill, 2018).

V souvislosti s probíhajícím konfliktem na Ukrajině zůstávají tyto snahy o expanzi BRICS stranou světové veřejnosti. Jak k tomuto problému napsal Prakash „*..Jak se ukrajinská válka zintenzivňuje, začal nový souboj o to, kdo povede svět. BRICS+ je první salvou v této nové bitvě o globální moc, ale určitě nebude poslední* (Prakash, 2022). Běloruska, Arménie, Kazachstánu, Kyrgyzstánu, Afghánistánu, Pákistánu, Nepálu Bhútánu, Vietnamu, Laosu, Kambodže, Brunei, Filipín, Malajsie, Indonésie, Thajska, Singapuru, Myanmaru, Srí Lanky, Bangladéše, Maledivy, Namibie, Botswany, Svazijska, Lesotha, Paraguaye, Venezuely Uruguaye a Argentíny. Tedy celkem 35 států, což představuje značnou jednací sílu.

23. května 2022 se konala virtuální konference BRICS Plus jako součást hlavního setkání s ministry zemí, včetně Spojených arabských emirátů, Saúdské Arábie, Egypta, Kazachstánu, Indonésie, Argentiny, Nigérie, Senegalu a Thajska. Čínské ministerstvo zahraničí po zasedání uvedlo, že „*Peking bude aktivně podporovat expanzi BRICS a přivítá další globální partnery, kteří se připojí ke skupině.* Mluvčí ministerstva zahraničí Wang Wenbin učinil tyto poznámky včera v prohlášení v reakci na otázky médií ohledně názoru Pekingu na rozšíření BRICS. *"Čína bude pracovat na stranách BRICS, aby pokračovaly v hlubokých diskusích o expanzi BRICS a určovaly standardy a postupy pro to na základě konsensu. Těšíme se, že se k velké rodině BRICS připojí další podobně smýšlející partneři,"* uvedl v prohlášení (Wang, 2022).

Dohody o zemích, které se budou moci připojit k organizaci, mohou být uzavřeny pouze po důkladných diskusích a postupech mezi členy BRICS, uvedli čínští odborníci a dodali, že současní členové G20, kteří mají zájem o vstup do BRICS, mohou být upřednostňováni a Indonésie a další rozvíjející se ekonomiky by mohly být pravděpodobnými kandidáty. Podle společného prohlášení ministrů, zveřejněném po zasedání, vyjádřili účastníci podporu diskusí

[2] Viz. Tasmin New Agency: *Iran Pledges Support for BRICS Goals*. [2022-06-25] Dostupné na: https://www.tasminnews.com/en/news/2022/06/25/2733774/iran-pledges-support-for-brics-goals

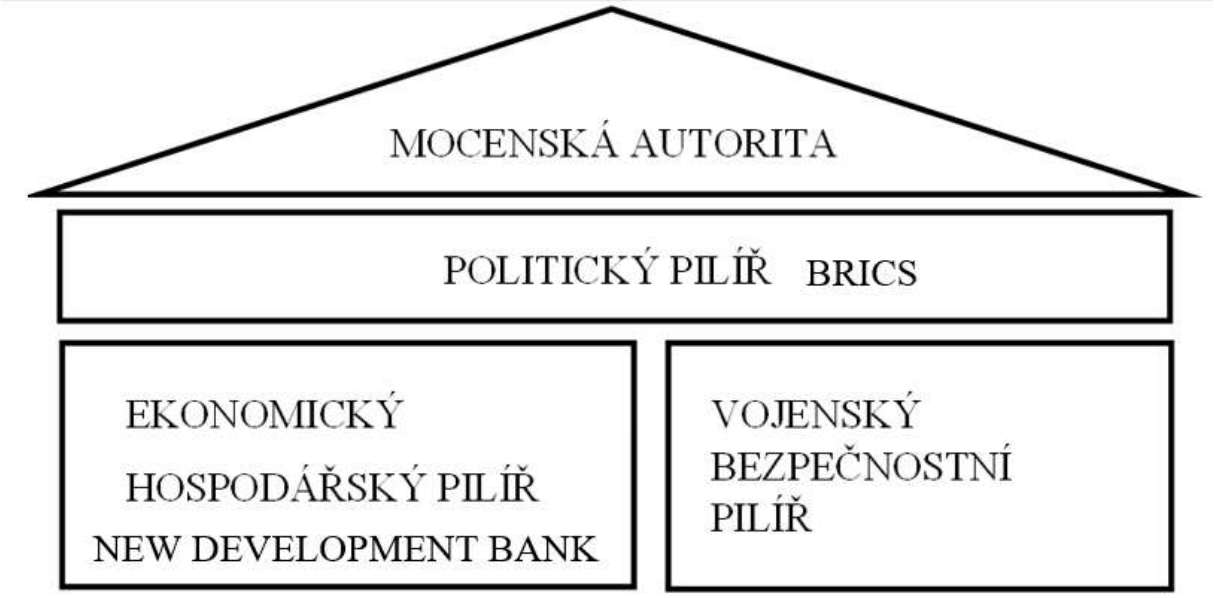
[3] Viz. LISSOVOLIK, J. *BRICS plus: Alternative globalization in the making.* [2018-01-21] World Economic Forum 2018. Dostupné na: https://www.weforum.org/agenda/2018/brics-plus-an-alternative-to-globalization-in-the-making/

mezi členy BRICS o procesu expanze a dohodli se na dalším vyjasnění hlavních zásad, standardů, kritérií a postupů pro tento proces expanze.[4]

4 NEW DEVELOPMENT BANK JAKO EKONOMICKÝ A HOSPODÁŘSKÝ PILÍŘ

Na čtvrtém summitu BRICS v Novém Dillí (2012) zvažovali vedoucí představitelé Brazílie, Ruska, Indie, Číny a Jižní Afriky možnost zřízení nové rozvojové banky, která by mobilizovala zdroje pro infrastrukturu a projekty udržitelného rozvoje v BRICS a dalších rozvíjejících se ekonomikách. , stejně jako v rozvojových zemích. Nařídili ministrům financí, aby prozkoumali proveditelnost a životaschopnost této iniciativy, zřídili společnou pracovní skupinu pro další studium a podali zprávu do příštího summitu v roce 2013.

Na základě zprávy ministrů financí na pátém summitu BRICS v Durbanu (2013) se lídři shodli na proveditelnosti zřízení Nové rozvojové banky a rozhodli se tak učinit. Bylo také dohodnuto, že počáteční příspěvek bance by měl být značný a dostatečný, aby byla efektivní při financování infrastruktury.



Obrázek 3 New Development Bank (NDB) jako ekonomický pilíř mocenské autority
Zdroj: autor

Během šestého summitu BRICS ve Fortaleze (2014) podepsali lídři Dohodu o založení Nové rozvojové banky (New Development Bank - NDB).

V deklaraci z Fortalezy vedoucí představitelé zdůraznili, že NDB posílí spolupráci mezi BRICS a doplní úsilí mnohostranných a regionálních finančních institucí o globální rozvoj, čímž přispěje ke kolektivním závazkům k dosažení cíle silného, udržitelného a vyváženého růstu.[5]

[4] Viz. Global Times: *BRICS will welcome news members, to better represent voices of emerging market: Experts.* [2022-05-21]. Dostupné na: https://www.globaltimes.cn/page/202205/1266202.shtml

[5] Dostupné na: https://www.ndb.int/about-us/essence/history/

Partnerství podporují plnění mandátu NDB tím, že posilují schopnost banky mobilizovat zdroje pro projekty infrastruktury a udržitelného rozvoje a zároveň podporují výměnu znalostí, lidských zdrojů a informací.

Jak uvádí například Luckhurst *„Návrh na vytvoření rozvojové banky BRICS byl představen na summitu v New Delhi v roce 2012. Tyto dohody a nahrazování dolaru národními měnami signalizují odklon od USA“* (Luckhurst, 2103).

Podepsáním dohody o sídle s vládou Čínské lidové republiky a memoranda o porozumění s šanghajskou městskou lidovou vládou dne 27. února 2016 se NDB stala plně funkční.

NDB dnes buduje robustní a diverzifikované portfolio projektů udržitelné infrastruktury, aby naplnila svůj mandát a dosáhla strategických cílů. Nová rozvojová banka rozvíjí svou činnost v souladu se svými cíli - zajistit zdroje pro financování infrastruktury a projektů udržitelného rozvoje v zemích BRICS a v dalších rozvíjejících se ekonomikách a rozvojových zemích. K naplnění svého účelu banka podporuje veřejné nebo soukromé projekty prostřednictvím úvěrů, záruk, majetkové účasti a dalších finančních nástrojů.

Činnost Nové rozvojové banky jako mezinárodní instituce se odehrává v souladu s cíli a principy Organizace spojených národů. V roce 2018 získala Nová rozvojová banka statut pozorovatele na Valném shromáždění OSN, čímž vytvořila základ pro možnost aktivní spolupráce v rámci mezinárodního společenství.

Na svém sedmém výročním zasedání, které se konalo 19. května 2022 Rada guvernérů NDB schválila **„Obecnou strategii banky na období 2022 – 2026“** s názvem „Zvýšení financování rozvoje pro udržitelnou budoucnost. Tato obecná strategie určuje další směr vývoje činnosti NDB. Strategie se zaměřuje na zlepšení schopnosti banky mobilizovat zdroje ve velkém, financovat diverzifikované typy projektů, využívat sofistikované nástroje, a budovat svůj robustní institucionální profil. Obecná strategie zahrnuje také konkrétní cíle, odrážející primární aspirace na dané období.[6]

Svou pozici silného hráče na světových finančních trzích upevňuje NDB také uzavíráním řady dohod o spolupráci, tzv. Memorand o porozumění, Dále se rozvíjela velmi intenzivně komunikace s Mezinárodními rozvojovými bankami. Celý proces od roku 2016 obsahuje následující partnerské vazby:

Tabulka 2 Vzájemné dohody NDB a mnohostranných rozvojových bank

Mezinárodní banka	Datum uzavření dohody
Skupina Světové banky	9. září 2016
Rozvojová banka Latinské Ameriky	9. září 2016
Mezinárodní investiční banka	1. Dubna 2017
Euroasijská rozvojová banka	1. Dubna 2017
Asijská banka pro investice do infrastruktury	1. Dubna 2017
Evropská investiční banka	1. Dubna 2017
Evropská banka pro obnovu a rozvoj	1. Dubna 2017
Finanční fond rozvoje povodí	26. dubna 2017
Mezi Americká rozvojová banka	19. dubna 2018
Africká rozvojová banka	18. října 2019
Mezinárodní banka pro rozvojovou spolupráci	28. června 2021
Asijská rozvojová banka	23. června 2022

Zdroj: autor podle www.ndb.int

[6] Viz. https://www.ndb.int/about-us/stategy/strategy

Není třeba nikterak zastírat, že vznik a činnost NDB je spojená se snahou o tzv. **„dedolarizací“,** která se objevila jako nová vlna v globálním obchodu poté, co některé země byly přesvědčeny o tom, že USA využívají dolar jako zbraň proti nepohodlným oponentům. Vážně se diskutuje o tom, že by roli dominantní měny, měla v závislosti na vývoji hospodářské situace převzít jiná měna, buď čínská nebo indická. Přinejmenším by měl být posílen jejich vliv.

V důsledku všech těchto aktivit postupně klesá podíl amerického dolaru na globálních devizových rezervách. V tomto smyslu také poslední summit BRICS dne 24. července 2022 projednával důležité okruhy problémů v této oblasti, jako jsou např. systém podmíněných rezervních ujednání, fungování platebního styku mezi zeměmi BRICS a vytvoření rezervní měny založené na koši měn zemí BRICS. Tyto problémy finanční architektury, budou v následujícím období tvořit základ jednání uvnitř NDB směrem k její mezinárodní emancipaci a posílení vlivu.

4.1 ROZŠÍŘENÍ NOVÉ ROZVOJOVÉ BANKY

K rozšiřování členské základny kromě samotného uskupení BRICS dochází také v rámci Nové rozvojové banky. K původním pěti zakládajícím členům se připojila další skupina zemí, čímž se zvýšila i autorita této instituce.

Jen za poslední dva roky přijala Nová rozvojová banka čtyři nové členy, kteří se budou dále podílet na její činnosti. Další kandidáti projevují živý zájem na budoucí spoluúčasti. Jde především o země uvedené v systému projektu BRICS+. Jedná se o Bangladéš, Spojené Arabské Emiráty, Uruguay a Egypt, všechny země byly přijaty v průběhu roku 2021.

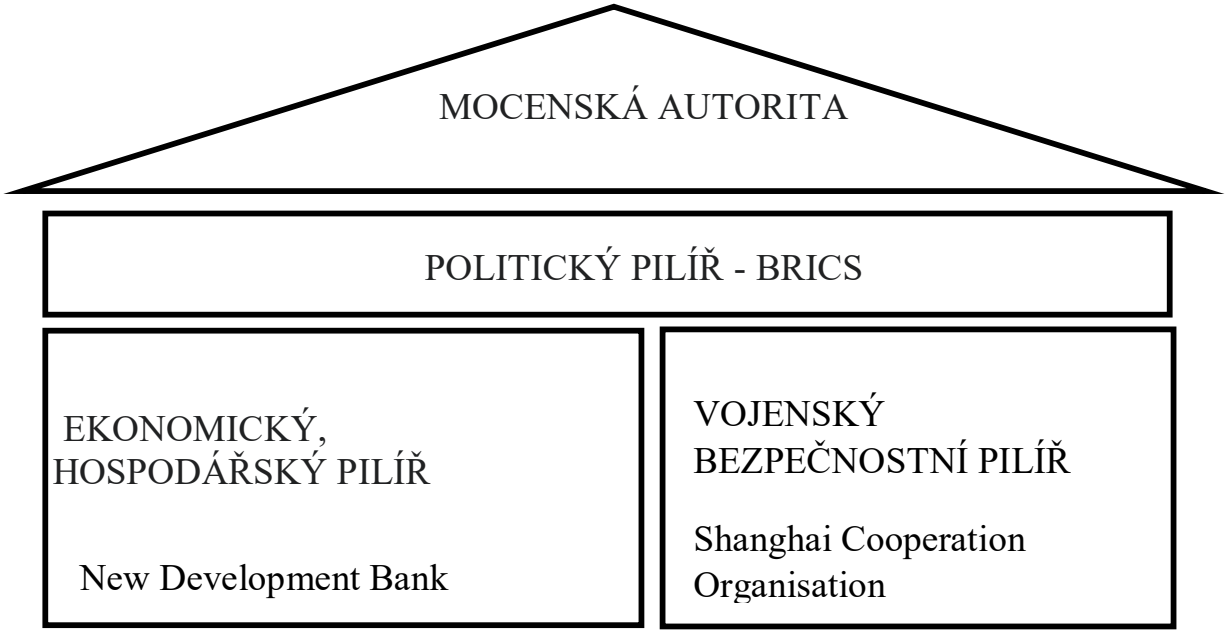
V následující tabulce je stručně uveden přehled členských zemí Nové rozvojové banky ke konci roku 2021.

Tabulka 2 Přehled členských zemí NDB k roku 2021

Členská země
Brazílie
Rusko
Indie
Čína
Jihoafrická republika
Bangladéš
Spojené arabské emiráty
Egypt
Uruquay

Zdroj: autor

5 ŠANGHAJSKÁ ORGANIZACE PRO SPOLUPRÁCI (SCO)



Obrázek 4 Shanghai Cooperation Orgaziation (SCO) jako bezpečnostní, vojenský pilíř mocenské autority
Zdroj: autor

Třetím pilířem, který tvoří strukturu konkrétní mocenské autority BRICS je Šanghajská organizace pro spolupráci (Shanghai Cooperation Organization – SCO) je stálá mezivládní organizace založená v Šanghaji dne 15. června 2001. SCO v současnosti zahrnuje osm členských států (Čína, Indie, Kazachstán, Kyrgyzstán, Rusko, Pákistán, Tádžikistán a Uzbekistán), čtyři pozorovatelské státy, které mají zájem o přistoupení. k plnému členství (Afghánistán, Bělorusko, Írán a Mongolsko) a šesti „partnerům dialogu“ (Arménie, Ázerbájdžán, Kambodža, Nepál, Srí Lanka a Turecko).

Charta Šanghajské organizace pro spolupráci byla podepsána na petrohradském summitu hlav států v červnu roku 2022 a vstoupila v platnost dne 19. září 2003. Jedná se o základní ustavující dokument, kde jsou stanoveny cíle a principy činnosti této organizace.

Od svého založení v roce 2001 se SCO zaměřuje především na regionální bezpečnostní otázky, svůj boj proti regionálnímu terorismu, etnickému separatismu a náboženskému extremismu.

Hlavními cíli SCO je posílení vzájemné důvěry a dobrých sousedských vztahů mezi členskými zeměmi; podpora efektivní spolupráce v politice, obchodu a ekonomice, vědě a technice, kultuře i vzdělávání, energetice, dopravě, cestovním ruchu, ochraně životního prostředí a dalších oblastech; společné úsilí k udržení a zajištění míru, bezpečnosti a stability v regionu a směřování k vytvoření nového, demokratického, spravedlivého a racionálního politického a ekonomického mezinárodního řádu. Charta Šanghajské organizace pro spolupráci byla podepsána na petrohradském summitu hlav států SCO v červnu 2002 a vstoupila v platnost dne 19. září 2003. Jedná se o základní ustavující dokument stanovující cíle a principy Organizace, její strukturu a hlavní oblasti činnosti.

Je to největší regionální organizace na světě, pokud jde o geografické pokrytí a populaci, pokrývající tři pětiny euroasijského kontinentu a téměř polovinu lidské populace.

SCO, často nazývaná "Východní aliance", si klade za cíl posílit důvěru a pocity sousedství mezi národními státy, podporovat spolupráci a spolupráci v otázkách bezpečnosti, obchodu, zpravodajství, technologií, výzkumu a kultury a kolektivně pracovat na boji proti třem zlům - **terorismu, separatismu a extremismu**.

Jednou z největších výzev, kterým SCO čelí, je nalezení způsobu, jak sladit rozdílné politické zájmy svých členských států. Tato organizace se vyvinula v regionální instituci s rozšiřujícím se seznamem formálních členů, pozorovatelských zemí a partnerů v dialogu.

Častým problémem je srovnání SCO a NATO. Zatímco tyto dvě organizace mohou mít překrývající se cíle, poslání a vize těchto organizací jsou výrazně odlišné. Zdá se, že NATO má globálnější zaměření, zatímco SCO se zdá být více znepokojeno vnitřními otázkami.

Na rozdíl od Atlantické aliance se SCO nikdy nezapojila do skutečné vojenské, protiteroristické nebo dokonce mírové operace. Vzhledem k tomu, že SCO postrádá stálé vojenské velitelské struktury a formace ve stylu NATO, ve skutečné krizi, která by vyžadovala jejich naléhavou vojenskou akci, by členové SCO museli dát dohromady intervenční síly založené s největší pravděpodobností na čínsko-ruské bilaterální dohodě.

Když byl na tiskové konferenci dotázán generální tajemník SCO Zhang Ming, zda lze rozšíření SCO srovnat s rozšířením NATO, Zhang řekl, že „*NATO je produktem studené války, zatímco SCO se liší v tom, že nejde o vojenskou alianci a tyto dvě organizace nelze srovnávat, neboť motivy, požadavky a důsledky způsobené těmito dvěma jsou podstatně odlišné.“* Z toho je patrně, že mezi oběma uskupeními nevládnou právě vztahy přátelství a důvěry a postoje Číny hrají v organizaci důležitou roli. Členské státy SCO se domnívají, že jejich vlastní bezpečnost nemůže být zaručena na úkor bezpečnosti jiných zemí. Zhang doufá, *že NATO se vážně zamyslí nad sebou samým a bude bojovat proti terorismu, nadnárodnímu zločinu, obchodování s lidmi a dalším otázkám jako svou prioritu. Teprve když NATO změní kurz a zaměří se na řešení těchto globálních výzev, bude SCO ochotna s ním zahájit dialog* (Zhang Ming, 2022)[7] a pozice Číny jako rodící se supervelmoci mají na SCO zřejmý vliv. Čínský prezident Si Ťin-pching prohlásil, že *„..země SCO by měly zůstat oddané duchu Šanghaje, usilovat o společnou, komplexní, kooperativní a udržitelnou bezpečnost, odmítnout mentalitu studené války a konfrontaci mezi bloky a postavit se proti praktikám hledání absolutní bezpečnosti na úkor sebe sama, ostatních, aby bylo dosaženo bezpečnosti všech* (Si ťing-pchin, 2019). Je zřejmé, že Čína a Rusko hledají novou geopolitickou agendu pro SCO. Čína byla vždy hlavním architektem ideologické základny této organizace. Nové mezinárodní prostředí a Čína jako reálná supervelmoc má na vývoj SCO rozhodující vliv.

Nestabilní regionální situace vyžaduje hlubší spolupráci v rámci SCO. V prvních letech SCO realita expanze NATO na východ a bující „tři zlé síly“ mimo jiné proměnily Šanghajskou pětku v mechanismus SCO. Barevné revoluce a ekonomické krize donutily členy SCO spojit se a spolupracovat. Nyní, kdy se zrychlují velké změny neviděné za celé století a pandemie zuří, vyvstávají vážné problémy pro domácí stabilitu a socioekonomický rozvoj členských států SCO. To posiluje povědomí o komunitě se sdílenou budoucností a podněcuje SCO k urychlení sebereformy, prohloubení spolupráce a výměn a zvýšení účasti na globálním řízení.

Jak uvedl Deng Hao *„V důsledku toho prochází SCO zásadní transformací a přechází od vnitřní spolupráce k vnitřní i vnější interakci, od bezpečnostní spolupráce k všestranné spolupráci a od regionální spolupráce k regionální správě. Výzvy SCO zahrnují vyvážení spravedlnosti s efektivitou, rozdíly v cílech hlavních zemí a vnější odpor, který vyžaduje, aby SCO zůstalo strategicky zaměřeno, drželo se orientace na problém, věnovalo pozornost podmínkám a postupovalo vpřed.*

[7] Zhang Ming, generální tajemník Šanghajské organizace pro spolupráci

Zatímco SCO obohacuje šanghajského ducha a podporuje principy neangažovanosti, nekonfrontace a necílení na jakoukoli třetí stranu, měla by pokročit s dobou v budování nového typu mezinárodních vztahů a společenství se společnou budoucností lidstva. Vize SCO o bezpečnosti, rozvoji, spolupráci, civilizaci a globální správě, která je široce uznávána svými členy pro svou klíčovou hodnotu pro novou éru, bude formovat „vědomí SCO“.

Dalším cílem SCO je zajištění soudržnosti prostřednictvím komunikace a vzájemné důvěry při respektování členské rozmanitosti, odlišností a zvolené cesty rozvoje, rovnosti velkých a malých zemí a konsensu mezi členskými státy prostřednictvím konzultací (Deng Hao, 2021)

Ačkoli ŠOS není výlučně vojenskou aliancí, její členské státy se účastní společných vojenských cvičení a válečných her. S indukcí Indie a Pákistánu mají čtyři členové SCO významné jaderné kapacity, což definitivně posílilo blok proti NATO. Ale ze všech členských států jen velmi málo splňuje požadavky NATO na vojenské výdaje (2% HDP), což vytváří velký tlak na několik vybraných zemí, aby nesly pochodeň během konfliktu. Navíc vzhledem k tomu, že členské státy nepřislíbily vojenskou podporu, mohly by svobodně odmítnout zapojení do budoucích vojenských konfliktů.

5.1 ROZŠÍŘENÍ ŠANGHAJSKÉ ORGANIZACE PRO SPOLUPRÁCI (SCO)

Vývoj SCO lze chápat z hlediska fází před a po roce 2017, kdy došlo k rozšíření členství. Zakládající fáze, 2001-2004, představila „Shanghai Spirit“ představující „vzájemnou důvěru, vzájemný prospěch, rovnost, konzultace, respekt ke kulturní rozmanitosti a snahu o společný rozvoj“. Za účelem vytvoření předpisů a právního základu se členské státy SCO dohodly na chartě, setkaly se na Šanghajské úmluvě o **boji proti třem silám zla** (terorismus, separatismus, extremismus) a schválily osnovu pro mnohostranný obchod.

Do roku 2004 byly zřízeny dvě stálé instituce, sekretariát v Pekingu a regionální protiteroristická struktura v Taškentu.

Fázi růstu SCO v letech 2004–2017 znamenala vnitřní výstavba a externí spolupráce. Vnitřní systém a mechanismus organizace byl postaven na Smlouvě o dlouhodobém dobrém sousedství, přátelství a spolupráci mezi členskými státy SCO, kterou podepsali hlavy států. Dokument z roku 2007 zakotvil v zákoně ideály trvalého přátelství a míru a upevnil konsensus členských států o rovném postavení a spolupráci. Úmluva proti terorismu z roku 2009 a Úmluva proti extremismu z roku 2017 konsolidovaly právní základ pro bezpečnostní spolupráci SCO a závazná mezivládní dohoda z roku 2014 o mezinárodním usnadnění silničního provozu posílila regionální spolupráci.

Strategie rozvoje SCO do roku 2025 potvrdila strategii a směr pro nadcházející desetiletí. Byly vytvořeny mechanismy pro formální setkání bezpečnostních tajemníků, pohraničních orgánů, ekonomických ministrů a ministrů pro pomoc při mimořádných událostech. Rada podnikatelů, byla zřízena mezibankovní asociace a fórum SCO. Vnitřní spolupráce zahrnovala to, že členské státy SCO na summitu v Astaně o Spojených státech a dalších zemích stanovily termín pro stažení svých vojenských základen ve Střední Asii. Společné protiteroristické vojenské cvičení Peace Mission se stalo pravidelným. Všechny zúčastněné strany podporují čínskou iniciativu Pás a stezka. Univerzita SCO je otevřena spolupráci ve vzdělávání.

Zásadní přelom v procesu rozšiřování SCO nastal v roce 2017, kdy se ve dnech 8. – 9. června v Astaně konalo historické zasedání Rady hlav států Šanghajské organizace pro spolupráci. Na zasedání byl udělen status řádného člena Organizace Indické republice a

Pákistánské islámské republice. To znamenalo první rozšíření členství SCO od jejího založení v roce 2001. Indie a Pákistán byly dříve přijaty jako pozorovatelé v roce 2005.

V roce 2021 bylo přijato rozhodnutí zahájit přístupový proces Íránu do SCO jako řádného člena a partnery pro dialog se staly Egypt, Katar a Saúdská Arábie. Co se týče Íránu, generální tajemník SCO Zhang Ming prohlásil, že *„Na základě Rozhodnutí Rady ministrů zahraničních věcí členských států SCO bude na summitu SCO v Samarkandu ve dnech 15. – 16. září 2022 rozhodnuto pověřit generálního tajemníka Šanghajské organizace pro spolupráci podpisem Memoranda o Závazky Íránské islámské republiky za účelem získání statutu členského státu SCO v Uzbekistánu, kde bude podepsáno první Memorandum o závazcích, pak v dubnu 2023 bude finalizováno," uvedla v úterý íránská ambasáda. exkluzivní odpověď na dotazy Global Times týkající se této záležitosti"* (Zhang Ming, 2022). Potenciál Íránu je výhodný pro všechny členy ŠOS, zvláště když se otevírá přístav Chabahar staví se jako brána na východ a na západ od Kaspického moře jako součást mezinárodního severojižního dopravního koridoru (INSTC). Chabahar na jedné straně spojuje Turkmenistán, Uzbekistán a Tádžikistán. Na druhé straně spojuje tyto země na západě s Ázerbájdžánem, Tureckem a Evropou a prostřednictvím íránského přístavu – s Afrikou a Indií.

Vstup do SCO je pro Raisiho vládu strategickým úspěchem. Klíčovými prioritami Raisiho zahraniční politiky je rozvoj, posilování a zlepšování vztahů s íránskými sousedy a asijskými zeměmi. Vstupem do SCO se do určité míry institucionalizují vztahy Íránu s asijskými mocnostmi, Ruskem, zeměmi Střední Asie a Pákistánem. SCO poskytne Teheránu důležitou příležitost vést pravidelný dialog s ostatními členy na různých summitech. Kromě toho bylo členství Íránu v organizaci interpretováno jako přání asijských mocností rozšířit spolupráci s Teheránem. Stálé členství v SCO znamená začátek nového multilateralismu v íránské zahraniční politice. Raisiho vláda prohlásila za své strategické priority kolektivní bezpečnost, multilateralismus a ekonomickou diplomacii (Shariathinia, 2021).

Generální tajemník SCO Zhangh Ming dále uvedl, že organizace obdržela oficiální žádost Běloruska o řádné členství v organizaci. Přijetí Běloruska ukázalo, že hodnoty, které organizace sleduje, jsou v souladu se zájmy této země. V současné době je Bělorusko pozorovatelským státem SCO.

Co se týče procesu expanze, jsou si odborníci vědomi také jistých problémů, které s sebou tento proces přináší. Jak uvádí Azhar Serikkajevová *„..na jedné straně rozšíření organizace zvyšuje její mezinárodní uznání a důvěryhodnost. Na druhé straně přináší výzvy související s vyhlídkami na integraci v rámci SCO a funkčnosti jejich institucí. Model SCO je však stále ve vývoji a budování a politická vůle členských států by mohla změnit strukturu organizace a její fungování. Je zřejmé, že zájem o SCO dne ode dne roste"* (Serikkajevová, 2022).

ZÁVĚR

Zkoumání podmínek mezinárodního vývoje je základním předpokladem pro možnost včas a odpovídajícími prostředky reagovat na možné situace, které by byly schopny ohrozit bezpečnostní stabilitu země.

Příspěvek se pokusil analyzovat alespoň v hrubých rysech pojem mocenské autority, protože i v systému mezinárodních vztahů jde o to, aby jednotlivé státy, jednotlivé klastry států, často se účelově spojujících, získávaly prostor pro realizaci svých zájmů, získávaly moc k jejich prosazení. V tomto pojetí je předkládána pilířová struktura vzniku, upevňování a kultivace mocenské autority v širším pojetí. Že tyto aspirace nemá jenom euroatlantická aliance, ale také skupiny států, které vyjadřují jistou nespokojenost s hegemonií takové moci v současném světě je v současnosti zřetelným faktem. Jedním z argumentů v tomto směru je skutečnost, že aktivity

zemí, nazývaných BRICS jsou přitažlivé pro další země a v rámci jednotlivých uvedených pilířů dochází k rozšiřování participace na cílech tohoto uskupení i dalšími státy.

V rámci analýzy je potřeba zkoumat názory a pohledy všech účastníků mezinárodních vztahů. V posledních letech dochází k dynamickým změnám v rozložení sil v rámci celosvětového společenství a přiložený text je jen snahou malou měrou přispět k objektivnímu poznání současné reality. Geopolitický, bezpečnostní význam Euroasie zůstává zatím poměrně v pozadí pozornosti odborníků, kdy se ovšem reálně projevuje vliv nově formované mocenské autority na tomto území. Jestliže chceme objektivně analyzovat novou dynamiku v oblasti mezinárodních vztahů, musíme se alespoň pokoušet slyšet a chápat argumenty i ostatních účastníků této mnohostranné interakce i když vychází z odlišných ideologických, kulturních a společenských podmínek. Pro společnou koexistenci je nezbytná snaha nacházet přijatelné kompromisy, zajišťující stabilní a mírový rozvoj lidské společnosti pro budoucnost.

Pokud jde o nově se formující mocenskou autoritu na území Euroasie, je zřejmé, že její politický, hospodářský a bezpečnostní vliv se bude stávat stále výraznějším. I přes vnitřní rozpory a skutečnost, že se jejich trajektorie vývoje ne vždy shodují jsou schopny prosadit svou vůli ve světovém společenství stále zřetelněji. Potravinová, energetická krize a probíhající válečné konflikty patrně tuto skutečnost dále zvýrazní. Státy s potenciálem produkce, ale také spotřeby na světových trzích se rozhodly svou politickou, ekonomickou a bezpečnostní emancipaci nejen deklarovat, ale také reálně prosazovat.

SEZNAM BIBLIOGRAFICKÝCH ODKAZŮ

ACHARYA, A. 2018. *Constructing Global Order: Agency and Change in World Politics* . Cambridge: Cambridge University Press.

ARIS, S. 2011. *Euroasian Regionalism: The Shanghai Cooperation Organisation.* Londýn: Palgrave Mac Millan. 223 p. ISBN 9781283210041

BÖRSEL, T. A. *The Myth of the Rising Powers.* In. Initiative on Foreign Affairs and International Relations. Dostupné na: https://ifair.eu/2012/05/01/the-myth-of-the-rising-powers/

DENG H. *20 Years of the SCO: Development, Experience and Future Direction. In: Contemporary International Relations, svazek 31 číslo 4 červenec/srpen 2021. Dostupné na: https://www.ciis.org.cn/english/ESEARCHPROJECTS/Articles/202112/t20211203_8276.html*

FREDHOLM, M. 2012 *The Shanghai Cooperation Organization and Euroasian Geopolitics: New Directions, perspectives and Challenges.* Copenhagen: Nordic Institute of Asian Studies

GIDDENS, A. 2013. *Sociologie (Sociology). 1. vyd.* Praha: Argo. 1052 s. ISBN 978-80-257-0807-1

JANDOUREK, J. 2003. *Úvod do sociologie. 2. vydání.* Praha: Portál, 232 s. ISBN 80-7178-749-3

KEOHANE, R. , O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press. 312 p.

KREJČÍ, O. 1997. *Mezinárodní politika.* Praha: Victoria Publishing 1997. ISBN 978-80-718-7034-0

Le TIAN: As India, Pakistan join SCO summit, what does its expansion mean? [2018-06-17] Dostupné na: https://news.cgtn.com/news/3d3d414e7a59544f77457a6333566d54/index.html

LUCKHURST, J. *Building Cooperation between the BRICS and Leading Industrialized States*. In. Latin American Policy. 2013, roč. 4, čís. 2, s. 251-268.

MJUMBDER, S. 2022 *De-Dollarization Paves Way for Stronger Rupee.* [2022-07-28] In. Euroasia News. 18. Dostupné na: Rupee Convertibility: De-Dollarization Paves Way For Stronger Rupee – Eurasia

PAVICEVIC, A. 2022 *BRICS Expansion: Five News Members in 2023?* In. Impaktor [2022-07-18]. Dostupné na https://www.impaktor.com/brics-expansion-five-news-members-in-2023

PRAKASH, A. *How an expanded BRICS could lead the world instead of the waning West.* [22-07-04] In. Infobrics.org. Dostupné na: https://www.scmp.com/comment/opiniwaning West.on/article/3183121/how-expanded-brics-could-lead-world-instead-waning-west

O´NEILL, J. 2018. *The „Next Eleven" and the World Economy.* In.: Project Syndycate [2018-04-18] Dostupné na: https://www.project-syndicate.org/commentary/n-11-global-economy-by-jim-o-neill-2018-04

SERIKKAJEVOVÁ, A. *Shanghai Cooperation Organisation: Risks of Expansion.* In: Euroasian Research Institute. Dostupné na https://www.eurasian-research.org/publication/shanghai-cooperation-organization-risks-of-expansion/ [cit. 22-08-18]

SHARIATHINIA Mohsen *Iran's full membership in the SCO: Stepping eastward.* In: MENAFFAIRS, The Middleeast, North Africa and Global Analyses [23.9.21]. Dostupné na: https://menaaffairs.com/irans-full-membership-in-the-sco-stepping-eastward/

THAROOR, S. *Rising Powers in Global Governance.* Marmara University. [2016-12-20]. Dostupné na: www.risingpowersproject.com

VINOKUROV, E. , LIBMAN, A. (2012). *Eurasian Integration: Challenges of Transcontinental Regionalism*. Basingstoke: Palgrave Mac Millan. p. 5

WEITZ, R. (2018). *The SCO and NATO Compared*. Dostupné na https://www.chinausfocus.com/peace-security/the-sco-and-nato-compared . [cit. 2019-03-18.

WANG, W. *BRICS group expected to expand – China*. In. Daily News.[30.05. 2022]. Dostupné na: https://www.msn.com/en-xl/asia/brics-group-expected-to-expand-china/ar-AAXRNbV

XINHUA (2018). *Full text of Chinese President Xi Jinping's speech at the 18th SCO Qingdao summit*. Retrieved from http://www.xinhuanet.com/english/2018-06/10/c_137244587.htm. Accessed on 10.01.2019.

ZAORÁLEK, L. *Ve stopách Trumpa. Přátelé a zájmy nejsou totéž.* In. Právo 11.3.2019. Dostupné na: https://www.cssd.cz/aktualne/blogy/ve-stopach-trumpa-pratele-a-zajmy-nejsou-totez/

ZHANG M. *SCO receives application from Belarus; its enlargement 'essentially different' from NATO expansion.* [22-07-15] In: Global Times. Dostupné na: https://www.globaltimes.cn/page/202207/1270644.shtml

Dr. Jindřich NOVÝ, Ph.D.
Policejní akademie České republiky Praha
Katedra managementu a informatiky
Lhotecká 559/7
143 01 Praha
E-mail: novy@polac.cz

REFUGEES AND THEIR PROTECTION - LEGAL AND INTERNATIONAL ASPECTS

Antoni OLAK, Bożena KONECKA-SZYDEŁKO, Maciej MARUSZAK

ABSTRACT

For many years, the refugee problem has been considered one of the important problems of modern society. The circumstances and reasons for the movement of refugees vary. Some are generated by situations that arise as part of interpersonal relationships or are the result of them (armed, racial and religious conflicts). Others are results beyond human control, such as natural disasters. The condition for preventing the influx of refugees and related solutions is respect for human rights. When solving the problems associated with the growing wave of refugees, it should be remembered that in the modern world a significant concept of security has changed, covering a wide range of problems, including environmental pollution, depletion of the Earth's natural resources, rapid population growth, proliferation of weapons, drug addiction, organized crime, international terrorism, human rights violations, unemployment, poverty, and mass migratory movements.

Keywords: Refugee, armed conflicts, respect for human rights

INTRODUCTION

The refugee problem is one of the pressing problems around which for many years there has been a fierce and unrelenting struggle for political, economic, national and other interests. When solving the problem of refugees and establishing legal protection measures, states are primarily guided by the need to respect human and civil rights and freedoms. The principle of respect for human rights is one of the fundamental principles of international law. Human rights are defined by economic, political, social, civil and cultural rights and freedoms. Provided by the law of the country where he lives. The nature of these rights and freedoms, as well as their scope, determine the socio-political considerations and the socio-economic structure of a given state and its legislation. The existence of such a category of people as refugees entails not only legal consequences for states, but also law and responsibility for their protection. Currently, this responsibility rests with the office of the United Nations High Commissioner for Refugees (UNHCR), who is the representative of the international community, but states can also perform refugee protection functions, although this is not always related to their material interests and, as a rule, they are reluctant to deal with this problem.

Before starting to define the concept of "refugee", it is necessary to define the concept of legal status. The legal status of a person is one of the types of social status and can be understood as a system of rights, freedoms, obligations, and responsibilities enshrined in law and guaranteed by the state, according to which an individual, as a subject of law (i.e. an individual with the personality legal) coordinates its behavior in society (Kazimierczuk, 2014, pp. 102-103).

The history of refugees goes back to antiquity: 695 BC. over 50,000 people took refuge in Egypt from the Assyrian army that conquered Judah. The process of the fall of the Roman Empire as a result of the Great Migration of Nations was caused precisely by the mass movements of people who could qualify for refugee status in our time. Viking raids caused over 40,000 inhabitants of the British Isles to flee to France in the 8th and 9th centuries (Banko, Nowak, Gatrell, 2022, pp. 1-3). The concept of "refugee" is in turn a kind of legal status. The

meaning of this concept, which appeared after the end of World War I, changed many times, which was caused by the gradual transformation of the refugee problem into a problem on a pan-European scale, and later worldwide, especially after the end of World War II (Florczak, 2014, p. 374).

The first attempts to define the concept of "refugee" in international law date back to the League of Nations. Treaties from that time are characterized by the extension of this concept to entire groups of foreigners who do not benefit from the protection of the country of origin (Sierpowski, 2002, pp. 198-207). This collective approach to the definition of the term "refugee" reflected the approach to solving refugee problems existing in the second quarter of the twentieth century in the form of the implementation by states of one-off actions aimed at solving crises causing the emergence of waves of refugees (Chrzanowska, Gracz, 2007,p. 31-39).

The term "refugee", formulated at the Geneva conference in 1926, was heavily politicized. At that time, the precondition for obtaining the refugee status was the presence of the person outside the country of origin and the person not enjoying the protection of the government of that country. It was only after the end of World War II that it was recognized that refugees were also people persecuted because of their religion, origin, social situation and other factors. The modern definition of the term "refugee" appeared only in the early 1950s. Pursuant to Art. 1 of the 1951 UN Convention Relating to the Status of Refugees, a refugee is "*a person who is outside his country of civil affiliation because of well-founded fears that he will be a victim of persecution on the basis of race, religion, citizenship, membership of a social group or political belief not the country's protection may or may not be used because of such concerns; Or, not having a certain citizenship and being outside the country of former habitual residence as a result of such events, maybe or not wanting to return to it because of such fears*".

B. Wierzbicki, analyzing and supplementing this concept, came to the conclusion that *"a refugee is a foreigner who - unlike other foreigners - has no normal ties to his own country,(...) which makes it impossible to benefit from the protection of any state. The distinguishing feature of a refugee is the motivation causing him to leave his own country or the motivation that prevents his return (...)*" (Wierzbicki, 1993, p. 26).

It can therefore be concluded that a refugee is a person who fled his country because he was disadvantaged there because of his race, religion, nationality, political opinion or belonging to a particular social group. For the same reasons, a refugee cannot return to his country. A person is a refugee even before the host country formally grants the application for international protection. This means that granting refugee status only officially confirms that a person is a refugee but is not the exact point in time when a person becomes a refugee (https://refugeesmigrants.un.org/definitions). From the above, it can also be concluded that refugees are persons who are entitled to legal protection within the framework and scope of the established in international legislation and the laws of individual countries (Jagielski, 2002, p. 159).

The most complicated step is to establish that the person has "legitimate fear" and that the person is "persecuted." In the first case, there are no formal mechanisms to verify the real situation of the refugee and the decision is often made on the basis of individual conclusions. To prove the presence of legitimate fear, the refugee should generally show that he is telling the truth. If the whole story of what happened is false, then usually (but not always) there will be no legitimate concern if the person returns to their country of nationality. Moreover, it should be proved that there is a real risk of the refugee returning to his home country. The meaning of the term "be persecuted" is not defined in the Refugee Convention itself. The lack of a formal definition allows a flexible approach to examining each individual application in line with changing conditions and the level of development of society (Jagielski, 2002, p. 159).

For a person to be considered a refugee, each of the five conditions listed should be met. For example, a person may have legitimate fear and not be able to obtain protection, but if they are not afraid of persecution for conventional reasons, they cannot legally be considered a refugee. Another person may meet all the other asylum criteria but be in a refugee camp in their own country. In this case, she is also not a refugee, and is instead referred to as "*an internally displaced person*" (Chrzanowska, Gracz, 2007, pp. 31-39).

Although the definition of "*refugee*" in the Convention is used by international organizations such as the United Nations, the term is still overused in the everyday lexicon. For example: in transmissions, the term "refugees" is often used to refer to people who have moved for economic reasons (labor migrants) and persecuted groups of people who remain in their own country without crossing the external border (internally displaced persons), (Chrzanowska, Gracz, 2007, pp. 31-39).

1 GENERAL RIGHTS AND OBLIGATIONS OF REFUGEES

Every asylum seeker, like refugees, has all the rights and fundamental freedoms as enshrined in international human rights treaties. This determines the close relationship between the issues related to refugee and the broadly understood protection of human rights. This in turn means that the work of the United Nations in the area of human rights and UNHCR work closely together in the protection of refugees, as each of these organizations strives to ensure the maximum protection of human dignity. International human rights instruments establish a minimum set of standards to ensure the dignity of treatment for human beings. These norms are formulated in many international documents of a universal and regional nature and concern fundamental issues of human rights. Moreover, in modern legal science, in the context of the development of the legal status of refugees in individual countries and international law, the improvement of the system of ensuring and protecting the rights of refugees, both the rights and obligations of people who have obtained this status are quite precisely defined by the norms of international law and the laws of individual countries (Chrzanowska, Gracz, 2007, pp. 31-39).

Refugees, like all other human beings, have certain rights. The most important international legal principle regarding the protection of refugees is the principle of non-discrimination, which guarantees that refugees have the right to enjoy the same basic rights and freedoms as citizens, even if they are not citizens of the host country (Kowalski, 2006, pp. 431-432). All rights promulgated in the International Charter of Human Rights, which includes the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, the International Covenant on Civil and Political Rights and the two Optional Protocols, belong equally to citizens, with the exception of certain rights, such as the right to vote. This means that even when they are outside their home country, refugees have the right to respect basic human rights. The International Charter of Human Rights contains many articles on the protection of the human rights of refugees in the country of asylum (Kowalski, 2006, pp. 431-432). Refugee rights can be divided into the following groups:

- Specific refugee rights under the Institute of International Defense,
- The rights that refugees enjoy on the same terms as the nationals of their host country,
- The rights that refugees enjoy on the same terms as foreigners living in their host country.

The first group includes rights that ensure the protection of refugees at the international level. One of such fundamental rights is laid down in Art. 14 of the Universal Declaration of Human Rights (1948), (https://www.unesco.pl/fileadmin/user_upl/pdf) right to asylum. Since a person should be legally residing in another country, they should additionally obtain a formal status allowing such stay or the right to move to a third country. Hence, it follows that the right

of refugees is the use of a lawful procedure to establish their status, as well as to obtain travel documents enabling travel to a third country (Kowalski, 2006, pp. 431-432). In addition, refugees have the right to a fair and lawful process for examining their refugee status applications. Consideration of the documents provided should take place within the framework of applicable law by authorized authorities, which should also help in collecting and preparing the necessary documents (Noll, Vedsted-Hansen, 1999, p. 363).

In a situation where the application of a person granting refugee status is rejected, he / she also has the right to appeal, which may be legally located in the host country (Noll, Vedsted-Hansen, 1999, p. 363). Pursuant to Article 3 of the 1951 Convention, refugees may not be discriminated against and should have equal rights with the nationals of their host country or at least with foreign nationals residing in that country. Consequently, welfare for refugees falls within the scope of national legislation, which in turn must be based on international standards. In particular, in accordance with the provisions of Chapter IV of the 1951 Convention, refugees should be granted the following social rights:

- supplying deficient products in the form of food rations,
- providing a place of residence,
- providing basic education,
- recognition of educational documents received by a refugee abroad,
- the right to a scholarship while studying at the university etc. (Convention Journal of Laws 1991 No.119, item 515).

Refugees have the same rights to work as nationals of their host countries. This applies to both access to jobs and payment of wages, as well as job durability, social benefits, etc. Pursuant to the law, refugees are also entitled to a retirement pension (Convention.... Journal of Laws of 1991, No. 119, item 515). Pursuant to Art. 15 of the Convention, refugees, together with other foreigners, have the right to form apolitical associations and non-profit trade unions. Refugees have the right to self-employment in agriculture, industry, crafts and trade, as well as the right to set up commercial and industrial enterprises on conditions no less favorable than those normally enjoyed by foreigners in the same circumstances.

In turn, the countries that acceded to the Convention undertake to:

- provide assistance to refugees residing on their territory in cases where they need help from a foreign country to which they cannot turn,
- grant refugees the right to choose their place of residence and freedom of movement within the country, provided that all rules applicable to foreigners are respected in the same circumstances,
- not to burden refugees with taxes and fees higher than those imposed under similar conditions and may be imposed on their citizens,
- allow refugees to take property brought with them on their territory to another country to which they have been allowed entry.

Granting refugees rights and freedoms is associated with many problems, as the authorities of some countries say that most asylum-seekers are in fact not refugees, but only economic migrants. For this reason, only 10-20% of those who apply for asylum receive refugee status (Krajewski, 2021, pp. 233-234). It should be added here that the arrival of refugees to their host countries takes place in waves, and modern refugee waves are very different from those that existed during the Second World War and were clearly political in nature. Currently, the reasons for the departure of refugees are different, as people run away from:

- civil wars and regional conflicts,
- violation of their rights and freedoms,
- aggression from the side of other countries or the occupation of their home country,

- poverty, epidemics, hunger, ecological disasters, etc (Cenda-Miedzińska,2012,149-151).

If you use the definition proposed by the United Nations, many of these people do not meet the definition of a refugee proposed by the United Nations, as a result of which some countries, especially in Latin America and Africa, to ensure the rights and freedoms of refugees, liberalize their legislation in such a way that it was possible to grant refugee status to a wider group of applicants. At the same time, in many other countries, applications for refugee status are still considered negatively if they do not provide political reasons for seeking asylum (Internal Displacement Monitoring Center, 2012, pp. 61-62).

From a human rights perspective, this situation is very worrying. It is not always possible to clearly distinguish between a refugee and an economic migrant. It is obvious that when it comes to the threat to life and freedom, the situation of a person at risk of starvation is not much different from that of another person who is at risk of arbitrary execution due to his political beliefs. Even without these considerations, the fact remains that whether a person is a refugee or economic migrant, national or non-citizen, or is leaving his country due to persecution, armed conflict, life-threatening or extreme poverty, he or she has the necessary minimum human rights and has the right to observe the minimum necessary standards of treatment (Cenda-Miedzińska, 2012, pp.151-153).

From the above, it can be concluded that despite the existing legal framework to protect the rights of refugees in this area, there are a number of problems. Therefore, the Organization of the Service for Refugees in terms of respecting their rights and freedoms is still poorly developed. *At present*, the greatest attention should be paid not only to the establishment of refugee status, but also to educational and information work; one the protection of refugee families is one of the serious problems which require special attention; *The other side* of the problem is that refugees and internally displaced persons often prefer to hide the obvious facts in the host country and are reluctant to contact the authorities for various reasons (Cenda-Miedzińska, 2012, pp.151-153).

2 THE HUMAN RIGHTS PROTECTION SYSTEM AND THE REFUGEE ASPECT

The concept of human rights appeared in the ancient era but was first explored and described in detail only in the 17th century by John Locke and Thomas Hobbes, who studied natural human rights. Since then, the understanding of human rights has deepened significantly, which resulted in the occurrence of different definitions (Tensey & Jackson, 2014, p. 61). The PWN encyclopedia states that human rights are "*basic, inalienable and universal rights of a person regardless of race, color, sex, language, religion, beliefs, national or social origin, property, birth, health and other*". In the documents of the international organization Amnesty International, Human Rights are defined as"*the basic norms that each of us enjoys resulting from the very fact of being human, eg the right to life, freedom of speech, association, or the right to education. The source of all rights and freedoms is the dignity of every human being*".

Both the first and second definitions can hardly be considered exhaustive as they are rather a listing of basic human rights without specifying their essence. M. Wasiński, who gave his own definition of human rights, tried to solve this problem with which these are "*certain freedoms (e.g. freedom of expression, freedom from torture, right to privacy, right to personal liberty) and privileges (e.g. to exercise electoral rights without any discrimination, to fair trial) which jointly fulfill the following conditions: they protect universally recognized goods (eg life, privacy), are guaranteed by the norms of positive law, are related to the dignity of the human person, and therefore have a natural, inalienable and universal character* ". As the concept of human rights is extremely broad, researchers are now talking about the existence of a whole system of human rights protection that operates at the interstate, state and and local. One of the

main principles of this system is the recognition that human rights are uni-versal. They apply to all people, they apply to all countries, regardless of whether the latter belongs to different international communities. Of course, the size and effectiveness of the exercise of rights and freedoms depends on many factors, and above all, the level of develop-ment of society as a whole. Secondly, human rights are in constant development, reflect the dynamics of social relations and increase the legal awareness of citizens (Wasiński, 2014, pp. 1-7).

Development of international cooperation in the field of consolidation and protection of rights and human freedom it ran in two ways. *The first* was characterized by the development and adoption of general and specific laws on the protection of human rights. *The second* is the cooperation of states in creating a real mechanism for the protection of human rights and monitoring their compliance (Wasiński, 2013/2014, pp. 1-7).

Many years of experience in the functioning of international organizations have shown that they are an indispensable element and an additional guarantee of the protection of human rights. They do not replace national authorities but complement them. One of the most important principles of contemporary international law is the principle of respect for human rights. On the other hand, the problem of ensuring and the protection of refugee rights appeared at the beginning of the 20th century, and they remain valid also in our times, and the human rights protection system, along with with refugees experiences many changes. Such an international system of human rights protection can be presented in the form of a diagram (Figure 1.).

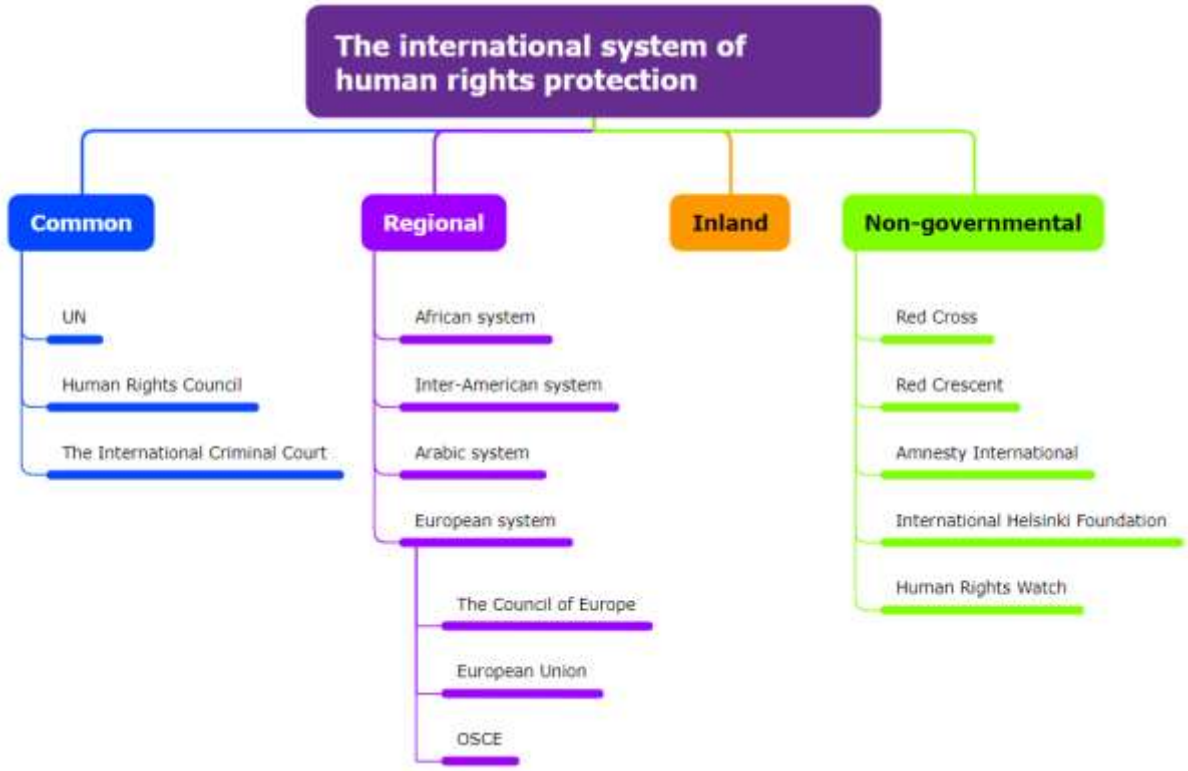


Figure 1 The international system of human rights protection
Source: https://www.na6.pl/wos/systemy_ochrony_praw_czlowieka

Millions of refugees registered in various parts of the world are the result of military inter-state conflicts, internal problems, systematic violations of human rights in some countries, etc. human rights to the lack of humanitarian aid (Grabowska-Bacza, 2015, pp. 38-39). Refugees trying to escape from war and persecution often find themselves in a very difficult

situation. They cannot enjoy the protection of their state. After all, it is often the case that their own country is threatened with persecution, and a person who has become a refugee is likely to maintain this status for many years. Will live in a refugee camp or illegally in a foreign country. As many as 70% of the refugees under the protection of the United Nations High Commissioner for Refugees (UNHCR) do not change their status for at least 5 years (UN High Commissioner for Refugees, 2022), so they systematically need protection and upholding their rights.

International protection within the framework shown in Figure 1. the system is a legal institution for people who, due to the danger, cannot return to their country. The concept of international protection covers two types of protection: refugee status and subsidiary protection.

The international legal standards for the protection of refugees are derived from international conventions, international customs and generalized principles that exist in major legal systems around the world. This international refugee law is designed to ensure equal and fair treatment of the most vulnerable to violation of the rights and freedoms of their group members. Therefore, such a law is closely related to international human rights law, the purpose of which is to protect the dignity and well-being of every human being. In international law, the share of human-oriented standards is constantly growing. These standards are based on the principle of respect for human rights and fundamental freedoms, which implies their general meaning:

- the promotion of rights and fundamental freedoms to all people without discrimination of any kind,
- the commitment of all states to act appropriately to ensure these rights,
- ensuring fundamental rights and freedoms both in normal life situations and in a state of emergency or armed conflict (Gholeh, 2015, pp. 51-53).

UNHCR is currently the primary organization in the system of international human rights protection specializing in the protection of refugee rights. Such protection should, by definition, be apolitical and impartial, and its only purpose should be to ensure the safety and well-being of refugees (Barycka, 2013, p. 116). In 1998, UNHCR recognized that the protection of refugee rights operated as part of the rights and obligations of the individual as well as the obligations of the state. International human rights law is a fundamental source of refugee protection principles and structures, complemented by refugee protection law (Note on International Protection ..., 1998).

The Human Rights Committee examines questions about state policy towards refugees but does not consider questions about specific refugees. Other bodies, such as the Committee against Torture, which is a supervisory body, may deal with individual cases but do not deal with the country's asylum policy in general. Therefore, some mechanisms are more appropriate for solving particular problems, while others are more suited to solving the problem as a whole (Łachacz, 2015, pp. 134-135). Mechanism for the protection of refugee rights in Europe, it is defined by the European Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950. According to this document, the primary authority responsible for ensuring compliance with the obligations entered into by States Parties to the Convention in the field of the protection of refugee rights is the European Court of Human Rights. This authority should also consider requests from citizens who are subject to the jurisdiction of the signatory states and have the right to apply to the Court for violation of their own rights set out in the Convention (Kowalski, 2006, p. 441).

3 VIOLATIONS OF REFUGEE RIGHTS

In today's world, the rule of sovereign states guarantees citizens that basic human rights are respected and protected, and that they are physically safe. But if someone leaves their country and becomes a refugee, these guarantees disappear. The legal status of such persons becomes questionable, and very often they are not protected by their own or even the host country, and as a result they are exposed to exploitation and other forms of abuse, as well as imprisonment and deportation. This process was particularly painful in the 21st century, when the number of refugees in the world becomes a record year every year (Figure 2).

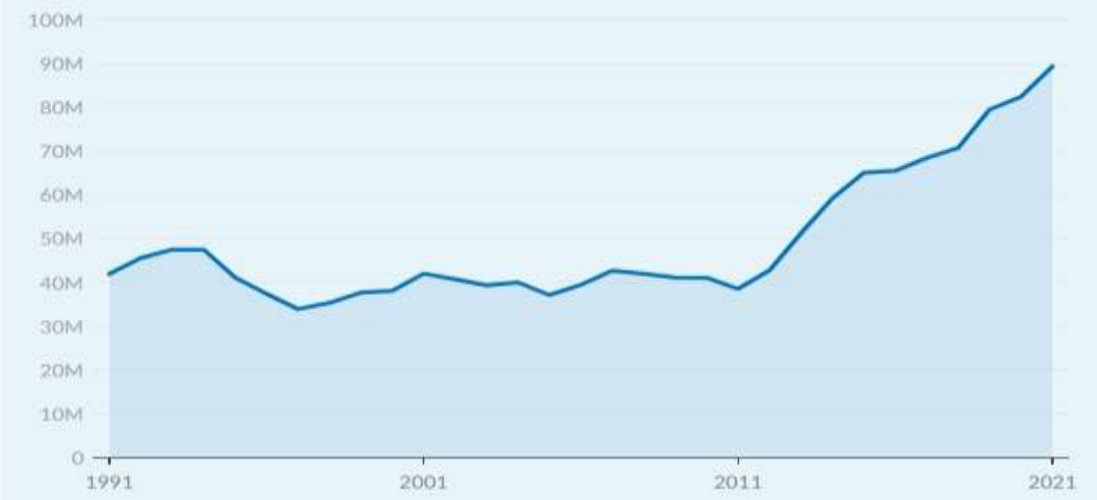


Figure 2 Number of refugees in the world in 1991-2021 according to UNCHR data
Source: Figures at a Glance, https://www.unhcr.org/figures-at-a-glance.html

Human rights violations are a major factor in the exodus of refugees as well as an obstacle to their safe and voluntary return home. Ensuring respect for human rights in the countries of origin is therefore of key importance both for the prevention and resolution of refugee problems. Respect for human rights is also essential for the protection of refugees in the countries of asylum (Mejsak, 2012, pp. 267-268). Refugees face human rights violations to a much greater extent than non-refugees. When applying for asylum, they are often subject to restrictions, for example preventing access to safe areas. They are often detained or forcibly returned to areas where their lives, freedom and safety are threatened. Many are attacked by armed groups or are recruited into armed forces where they are forced to fight on one side or the other in domestic conflicts. Asylum seekers and refugees are also often victims of the worst manifestations of racism (https://www.hfhr.pl/granica-praw-czlowieka-przepkuje-organ.-spoleczne-przep).

Asylum seekers' problems do not end when they finally cross the border of their destination country and go through the first phase of their asylum application (already at this stage they are often detained and questioned). When examining applications for asylum, and even after obtaining refugee status, they may face numerous limitations and obstacles.

In some regions, they are subjected to torture and degrading treatment. There are also cases when their refugees were denied access to courts and legal protection, and moreover, a large part of refugees are unable to find a job, start a business, obtain legal aid, etc. As a result, even if a refugee is not forcibly sent away from the country, which he initially intended to

become, may feel forced to leave him because of the restriction of his rights and freedoms, and thus the impossibility of leading a dignified life.

For example: thousands of refugees and migrants die or suffer serious human rights violations when traveling between West and East Africa and the European Mediterranean coast. Different groups of people can be the perpetrators of physical violence (Figure 3.), Which makes it difficult both to ensure the rights and freedoms of refugees and to prevent their violation.

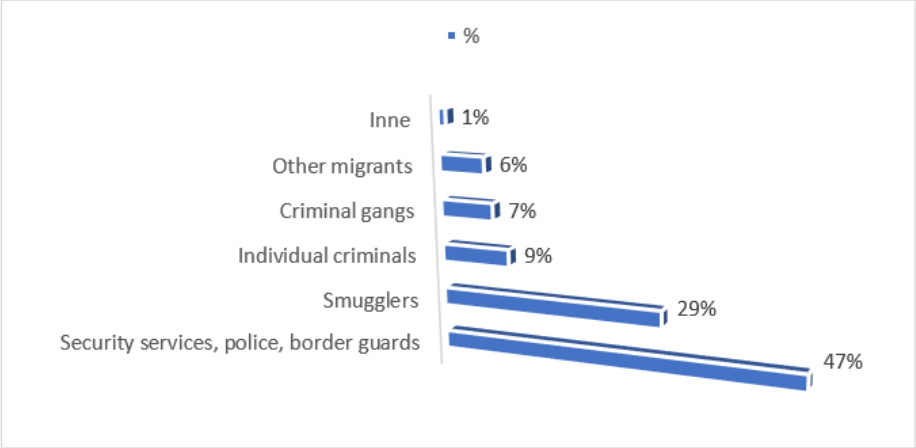


Figure 3 Perpetrators of physical violence against refugees in the Mediterranean region
Source: own study based on *On this journey, no one cares if you live or die. 'Abuse, protection,and justice along routes between East and West Africa and Africa's Mediterranean coast*, UNCHR 2020, p. 21.

As the chart above shows, protection of the rights of refugees, especially those from Asia and Africa, is also difficult due to the fact that they are most often violated by employees of state services whose task is to protect such rights. The problems of violating the rights of refugees concern not only African and Asian countries, but also the European Union. For example, according to data from the Center for Equal Opportunities and Combating Racism in Belgium, in 2013, 80% of all religious discrimination cases are related to Muslims or Muslim associations, of which: 51% are cases of discrimination in the media (racist websites, statements on forums and social media, etc.); in 19% of cases it is discrimination in the professional sphere; 11% of cases concern discrimination in education.

It should also be stated that the violation of the rights of refugees occurs at each stage of their displacement:

- in the countries of origin where violation of refugee rights is the prime reason for their resettlement,
- in countries through which refugees' pass / transit,
- in the countries of destination.

The plight of refugees has been made worse by the pandemic Covid-19. In many countries, the processing of asylum applications has been delayed, and many refugees and migrants were particularly vulnerable to living in the overpopulated and unsanitary conditions. The pace at which governments have planned to reduce greenhouse gas emissions will not avoid the worst human rights effects of the climate crisis. Interference with the European legal framework in the field of human rights has not stopped. States continued to trade arms with Saudi Arabia and the United Arab Emirates (UAE), despite the risk of human rights violations during the conflict in Yemen.

SUMMARY

Increasingly, mass displacements are not only the result of armed conflict, but also the result of ethnic cleansing and a sharp deterioration in the social situation. As a result, states frequently refuse these persons asylum on the basis of their failure to meet the criteria and grounds for persecution set out in the 1951 Convention Relating to the Status of Refugees. On this basis, it can be concluded that the main document to date on the definition of the status of refugees and their legal protection, namely the Convention on the Status of Refugees of 1951, requires revision and improvement.

Although regional agreements have been concluded between European countries which define the countries responsible for examining applications for refugee status, their national laws often contradict each other. This circumstance is often the reason for refusing asylum, and the person concerned is prevented from applying for asylum in another country.

Significant progress has been made over the past 40 years in the development of international instruments regulating the status and treatment of refugees. It is now necessary to focus on the implementation of these instruments at international, regional and national levels.

The system of modern international cooperation on refugees is not fully unified, on the contrary - it consists of several systems, sometimes not linked by international legal agreements, having their own distinct features and characteristics, and at the same time insufficiently coordinated. It cannot be categorically stated that the above-mentioned cooperation systems do not interact with each other at all and are completely closed. It is clear, however, that poor cooperation is one of the many causes of ineffective international cooperation on the refugee issue, which in turn has a negative impact on the overall situation of refugees in the world.

When solving problems related to the increasing wave of refugees, it should be remembered that in the modern world the very concept of security has changed, which covers a wide range of problems, including environmental pollution, depletion of the Earth's natural resources, rapid population growth, proliferation of weapons, drug addiction, crime organized, international terrorism, human rights abuses, unemployment, poverty and mass migratory movements. These and other problems can cause the increasing waves of refugees, so there is a need to adapt modern law both in terms of defining such people and giving them the necessary assistance and protection.

BIBLIOGRAPHY

BANKO, L. – NOWAK, K. – GATRELL, P. 2022. What is refugee history, now? In *Journal of Global History*, Volume 17, Issue 1, p. 1-3. ISSN: 1740-0228.

BARYCKA, K. 2003. Rights of refugees in armed conflicts in the international system of human rights protection, Armed conflicts and international disputes on the threshold of the 21st century, Wroclaw, p. 116. ISBN: 83-88555-95-2.

CENDA-MIEDZIŃSKA, K. 2012. Legal and social aspects of refugee safety, Colloquium of the Faculty of Humanities and Social Sciences, Quarterly, No. 3, pp. 149-151, ISSN: 2081-3813.

Convention Relating to the Status of Refugees, Geneva, 28 July 1951, Journal of Laws 1991, no.119, item. 515. [online], https://www.unhcr.org/4d934f5f9.pdf, [access: 17/05/2022].

COVID-19 and human rights, [online] https://amnesty.pl/covid-19-i-prawa-czlowieka/, [access: 21. 06. 2022].

CHRZANOWSKA, A. – GRACZ, K. 2007. *Refugees in Poland. Cultural and legal barriers in the adaptation process, Association of Legal Intervention*, Warsaw 2007, pp. 31-39. [online] http: // libr. Sejm. gov.pl/tek01/txt/onz/1951-b.html, [access: 10/08/2022].

GHOLEH, M. 2015. The legal and factual situation of refugees and human rights In *International protection of human rights - contemporary problems in the world*, Ed. UW, Wroclaw , pp. 51-53, ISBN 978-83-61370-59-8.

GRABOWSKA – BACZA, A. 2015. Human rights during the war. In *Student Scientific Papers*, Lublin, Issue 26, year XVIII, pp. 38-39, ISSN: 1506-8285.

KAZIMIERCZUK, M. 2014. The concept, essence and source of freedom and human rights. In *Legal studies*, 2014, No. 26, pp. 102-103, ISSN: 1644-0412.

KOWALSKI, M. 2006. Between discretion and obligation: the foundations of the legal and international protection of refugees, In *Politeja*, No. 1 (5), pp. 431-432, 441, ISSN**:** 17336716.

KRAJEWSKI, P. 2021. Interpretative and legal problems of the definition and status of environ mental migrants, In *Legal and political studies*, No. 54, pp. 233-234, https://doi. org/ 10.31648/sp.7178.

MEJSAK, R. 2012. The system of refugee protection in the universal dimension - institutional and legal perspective, In *Podlaska Studies*, No. 20, pp. 267-268, ISSN:0867-1370.

NOLL, G. - VEDSTED-HANSEN, J. Non-Communitarians: Refugee and Asylum Policies, In *The EU and Human Rights, eds. P. Alston*, Oxford 1999, p. 363, ISBN:0-19-829806-4. Florczak A., Refugee, 2014, [in:] *International organizations in action*, OTO, Wroclaw, p. 374, ISBN 978-83-927859-8-9.

JAGIELSKI, J. 2002. Selected administrative and legal aspects of refugee issues in Poland, In *Protection of refugees. Tenth anniversary of Poland's accession to the Geneva Convention, Ministry of Foreign Affairs* Warsaw, p. 159, ISSN: 2300-2891.

ŁACHACZ, O. 2015. The principle of non-refoulement in international refugee law - an international custom or a peremptory norm of international law? In *Problems of contemporary international and comparative law*, No. 15, pp. 134-135, ISSN: 1730- 4504.

SIERPOWSKI, S. 2002. Matters of refugees in the activities of the League of Nations, In *Visions and reality.* Studies on society, economy and politics, UAM, Poznan, pp. 198-207, ISSN:1234-2041.

TANSEY, N. – JACKSON, N. 2014. Politics: The Basics, Routledge, London and New York, pp. 61. ISBN 9780415841429.

WIERZBICKI, B. 1993. Refugees in international law, WN, Warsaw 1993, p. 26, TIN: T01106292.

WASIŃSKI, M. 2013/2014. The contemporary meaning of the term: human rights, In *Historical and theoretical foundations of human rights*, PWN, No. 1, pp. 1-7. ISBN:978-83-937983-2-2.

prof. nzw. dr hab. Antoni OLAK, MBA
State Higher School of Technology and Economics in Jarosław
University of Entrepreneurship and Administration in Lublin
Poland
E-mail: antonio130@vp.pl

Mgr. Bozena KONECNA-SZYDELKO
Provincial and Epidemiological Station in Rzeszów
UMB v Banskej Bystrici, Department to International Relations
Slovak Republic
E-mail: bkszydelko@op.pl

Mgr. Inź. Maciej MARUSZAK
Podkarpacki Regional Branch of the Polish Red Cross
UMB v Banskej Bystrici, Department to International Relations
Slovak Republic
E-mail: maciejmaruszak@gmail.com

KULTIVÁCIA ČLOVEKA 21. STOROČIA - POZITÍVNA EDUKÁCIA

THE CULTIVATION OF MAN OF THE 21ST CENTURY - POSITIVE EDUCATION

Mária PETRUFOVÁ

ABSTRACT

The author of the article points out the necessity of applying a positive approach to education by linking pedagogy, didactics, psychology as well as the theory of education to the cultivation of a person even in the conditions of military institutions. The pedagogic-didactic transformation of the teacher's work is gradually shifting from a directive, transmissive approach to students - college cadets to activating and motivating teaching - which naturally enables the positive psychology movement.

Keywords: positive psychology, education and positive motivation, teacher and student self-regulation, positive attitude towards education

ÚVOD

Ak chceme kvalitnejšie pripravovať študentov na život je potrebné aplikovať do edukačného procesu prvky hnutia pozitívnej psychológie. Svet je čím ďalej tým zložitejší a zvýšený výskyt nežiaducich foriem správania, neustály tlak na výkony ľudí a pocit zbytočnosti v procese neustálych zmien vyžaduje vyhľadávať alternatívne prístupy a prijímanie nových filozofii v edukácii v akomkoľvek type vzdelávania. Je potrebné viac ako kedykoľvek predtým sa snažiť uplatňovanie aktivizujúcich metód a foriem aj vo vojenskej edukácii. Snahou všetkých aktérov v edukácii by mala byť efektívna snaha o maximálnu aktivitu a zapojenie študentov do edukačných procesov. Edukácia by mala viesť k k emocionálnej spokojnosti v plnohodnotnom živote všetkých nás – detí, mládeže ako aj dospelých.

1 HNUTIE POZITÍVNEJ PSYCHOLÓGIE

Z histórie ale aj z predchádzajúcich pedagogických teórii je dnes často považované za nedostatok v súčasnej edukácii, ktorá bola a aj ešte dnes je často založená na direktívnom a neomylnom prístupe učiteľa – pedagóga na obsahovú-procesuálnu stránku vyučovania bez možnosti väčšej aktivizácie a aktivity študenta – uplatňovanie tzv. transmisivného vyučovacieho štýlu.

Mnoho učiteľov a lektorov vo svoje didaktickej praxi aplikuje len niektoré vybrané prvky alternatívneho prístupu, nových filozofii a hlavne sa ešte aj dnes málo učiteľov snaží o zatraktívnenie a zefektívnenie edukačného procesu. Hnutie pozitívnej psychológie sa zaoberá princípmi pozitívnej psychológie a vedecky študuje:

- rôzne emocionálne, intelektové a sociálne oblasti ľudského žitia,
- vplyv na spokojne prežívanie v súlade s túžbou po poznaní, láske múdrosti, pravde, šťastí, po úspechu a určovaní aj dosahovaní osobných životných cieľov.

  Uplatňovaním pozitívnej psychológie v edukácii sa aktéri snažia dospieť k emocionálnej spokojnosti v plnohodnotnom živote (Valjentová, 2020).

Pozitívna psychológia pristupuje vedecky k skúmaniu ľudského myslenia, prežívania emócii a správania, zdôrazňuje silné stránky, miesto zamerania sa na tie slabé a budovane toho dobrého v živote, miesto naprávania toho zlého. (Hanuliaková, 2022, s.11).

Vedecké a odborné hnutia pozitívnej psychológie vzniklo ako rekcia na skutočnosť všeobecného uprednostňovania negatívnych javov života a problémových oblasti psychiky. Cieľom je charakterizovať nosné ciele pozitívnej spokojnosti človeka v živote, aby život nebol len obyčajné prežívanie, ale kvalitné žitie (Seligman 2014, Peterson, 2004). Podľa uvedených autorov sú kladné pocity ako radosť, humor, optimizmus, podpora silných stránok osobnosti, záujem o činnosť ako takú identifikujú úspech a rozvíjajú ľudskú potencialitu a rozmanitosť, sebarealizáciu, pozitívne sociálne vzťahy, spoločnosť charakterizovanú láskou, úprimnosťou, spolupatričnosťou, nádejou, vďačnosťou tvoria možnosti obsahu potrebného pre zdravú ľudskú prosperitu.

Vychádzajúc z týchto názorov ***pozitívna psychológia sa sústreďuje na pochopenie duševného života*** (strádania a odstraňovania vplyvov) , ktoré daný stav spôsobujú. Mala by ich robiť šťastnejšími a eliminovať negatívne vplyvy na duševné zdravie človeka***. Jedná sa o vedu študujúcu rozvoj potenciálu a super dispozícii osobnosti človeka, spolu s budovaním najlepších životných vlastností pre kvalitné žitie*** (Seligman 2012). Ak by sme to chceli zľahčiť tak obsahom pojmu pozitívna psychológia sú subkategórie: šťastie, láska vďačnosť, optimizmus, nádej, charakter, životná činorodosť, zmysluplnosť okamihov žitia, obohacuje vzťahy medzi ľuďmi, čo predstavu základ pre optimálny ľudský rozvoj v súčasnej modernej dobe (Hanuliakova, 2021).

1.1 POZITÍVNA EDUKÁCIA A POSTAVENIE UČITEĽA V NEJ

Pozitívna edukácia nadväzuje na teórie a výskumy odborníkov hnutia pozitívne psychológie (Seligman, Czikszentmihályi, Fredricksonová, Lyubomirský, Ed Diener a i.) V zmysle hesla „Dobrá škola nie je zameraná len na to, aby žiaci dosiahli akademický potenciál, ale zacieľuje sa tiež na rozvíjanie osobnosti študentov ako starostlivo zodpovedných a v konečnom dôsledku ako produktívnych a platných členov v spoločnosti a v živote“. *Pozitívne vzdelanie – edukácia sa len okrajovo dostavajú do každodennej činnosti učiteľov a študentov* – ich hlavnou úlohou je najmä blahobyt, ktorý podporuje vzdelanie a rozvíja ich ako dobrých ľudí a občanov.

V tomto kontexte možno dnes definovať ***„pozitívnu edukáciu ako vzdelávanie pre tradičné životné zručnosti a edukácia k šťastnému človeku***“. Malo by byť založené na tých najlepších výučbových stratégiách a s cieľom pomôcť študentom dosiahnuť najlepšie vzdelávacie výsledky spárované s aspektmi pozitívnej psychológie – zabezpečujúcich bezpečnosť a blaho študentov. Napriek tomu že je to mladá veda, svojím vedeckým prístupom, analýzami a závermi spĺňa požiadavka súčasnej edukácie študentov.

Klasici v pedagogike hovoria, že učitelia sú v rámci vyučovacej činnosti mnohokrát orientovaní primárne na sprostredkovanie čo najväčšieho obsahu učiva, jeho preverovanie a hodnotenie zvládnutia študentmi. Oveľa menej priestoru vytvárajú ***na podporu a rozvoj emócii., ktoré budú študentov sprevádzať celý život a s ktorými sa musia naučiť pracovať. Preto málo pozornosti venujú pripravenosti a neschopnosti projektovať vyučovaciu jednotku tak, aby mohol učiteľ pracovať so žiačkami emóciami a emóciami triedy ako kolektívu, tímu a so sociálnou dimenziou prostredia študijnej skupiny***. *(Hanuliakova.,2022, s.12).*

Nie je to nový názor, lebo prof. Zelina aplikoval tieto myšlienky prístupy do školy, do edukácie už v roku 2016 (Zelina 2016, s.21) a zhrnul ich do nasledovných oblastí:

- **Kognitívny rozvoj žiaka**: (mať radosť z učenia, myslenia a z objavovania nových poznatkov a riešenia problémov) z toho vyplýva aj iný prístup učiteľa – oceňovať poznanie, využívať problémové a heuristické metódy a projektové vyučovanie,

uplatňovať stratégie metakognície a auteragulatívneho učenia, orientovať sa na múdrosť žiaka, schopnosť klásť si ciele, optimizmus a životnú pohodu.

- **Pozitívne emócie**: žiak má rád školu, učenie teší sa do školy, má dobré pocity z toho čo sa učí, dobre sa cíti medzi spolužiakmi aj napriek zlyhaniu, sklamaniu, strachu, napätie). Z toho vyplýva prístup učiteľa – prežívanie emocionálnych zážitkov, emocionálnej tvorivosti, kladné seboceňovanie, inscenačné metódy tvorivá dramatika a rôzne terapeutické postupy.
- **Pozitívna motivácia:** žiak je vedený k zmyslu života, k všeľudským hodnotám a z toho vyplýva prístup učiteľa – apelovanie na pozitívne hodnoty, vzťah k školským hodnotám, stratégie, ktoré eliminujú vyhorenie žiakov, nechuť sa učiť, rezignácia, ľahostajnosť, nezáujem, agresia, absencia viery, presvedčenia a hodnoty.
- **Pozitívna socializácia**: sú tu posilňované tie stránky osobnosti, ktoré vytvárajú produktívne medziľudské vzťahy a z toho vyplývajú prístupy učiteľa: viesť žiakov k solidarite, tolerancii, pomoci, tvoriť pozitívnu atmosféru a klímu v trieda, kvalitné vzťahy, pozitívna triedna klíma znižuje neochotu spolupracovať, nenávisť, egoizmus, podporuje schopnosť tolerovať ľudí.
- **Autoregulácia**: žiaci sa učia samostatnosti, sebariadeniu, disciplíne a zodpovednosti a z toho vyplýva aj prístup učiteľa viesť žiakov k samostatnosti, čo vedia urobiť sami, urobia samostatne, ovládať svojej myslenie, sústredenosť, pozornosť, vytrvalosť, ovládať svoje emócie, strach, zlosť, zlú náladu, psychomotorická kontrola
- **Potencionality pre život**: pozitívny postoj k vzdelávaniu je nevyhnutnou podmienkou CŽV, postoj k rekvalifikáciám v rámci pracovných príležitostí, zvyšovanie si kvalifikácie, samo štúdium, doplňujúce informálne a neformálne vzdelávanie. A z toho vyplývajúci prístup učiteľa: podporovať tvorbu postojov, hodnôt vo vzťahu k morálnym aspektom, k pravidlám života a k spoločnosti, učiť žiakov verbalizovať vlastné pocity a emócie v rodinných , partnerských a v rôznych životných situáciách, cvičiť sociálne zručnosti pri zvládaní a riešení náročných situácii a úloh, motivovať žiakov k aktívnej účasti v dobrovoľníctve, charite a prosociálneho správania – vedieť si určiť poradie životných a pracovných cieľov, denný režim, viesť ich k životnej sebadisciplíne.

Pozitívna edukácia sa musí orientovať na prípravu človeka, ktorý bude: flexibilný, schopný reflektovať na nové poznatky, podnety a výzvy, pripravený riešiť konflikty, znalý cudzích jazykov a pripravený na život mimo blízkej lokality. To aby prvky pozitívnej psychológie v edukačnej praxi boli dostupne a prakticky realizovateľne musí vedenie škôl na širšej úrovni v širšom kontexte prijať a riešiť pozitívnu edukáciu v úzkej spoluprácu so školskými psychológmi. To zároveň budovať pozitívny model školy podporujúcej sily, prednosti, potenciality jednotlivcov a iniciovať výraznú zmenu v riešení negatívnych javov k rozvíjaniu najlepších kvalít školy ako inštitúcie a ľudí v nej. Pretože človek budúcnosti by mal byť nielen výkonný, ale aj šťastný.

V edukačnom procese sa dnes už zdôrazňuje, že okrem vzdelania, učenia, ovládania základných poznatkov, vedomostí zároveň treba zušľachťovanie mimo výkonnostných charakteristík študentov – emócií, citov, socializácie, hodnôt, samostatnosti, tvorivosti a motivácie v aktuálne pozitívnej študijnej a školskej klíme

Dnes už vieme s istou povedať, že už existuje priamapozitívna korelácia medzi pozitívnou školskou klímou a zlepšujúcimi s výsledkami učenia a úspechu študentov. Aj keď ***činitele pozitívnej klímy*** sú stále predmetom skúmania, poriadku, bezpečnosti, disciplíny vzťahov medzi učiteľmi a študentmi, férovosti a jasnosti pravidiel v škole. Klíma by mala mal motivovať aj zapájať do výučby aj zamestnancov školy a odstraňovať prekážky pri učení a vytvárať vhodné podmienky pre učenie, súdržnosť a fungovanie každej vzdelávacej inštitúcie. Pozitívna školská klíma pomáha napĺňať vývinové potreby učenia študentov, ak majú

pocit, že je o nich postarané, sú vhodne podporovaní v proces učenia sa - tým sa rozvíja prepojenosť so školou a praxou., vzdelanostná ašpirácia a výkon (Kantorová, 2015) Ak je ***školská klíma a triedna klíma negatívne ovplyvnená- prejavujú sa v nej nasledujúce javy:*** stresory, strach ako aj konflikty, prehnané nároky učiteľov, zamestnávateľov priestorové a materiálno- technické nedostatky vo vyučovacom priestore a preplnené kurikulá predmetov. Dobré podmienky v edukácii majú veľký vplyv a zároveň pôsobia aj na sebahodnotenie študenta (Petlák 2020).

Na základe mnohých analýz vypracovali veci oblasti pozitívnej klímy školy. (Blaštíková 2018) spracovala ***päť oblastí ich dimenzie pre pozitívnu klímu školy*** podľa National School Center (2017): bezpečie, vyučovanie a učenie, interpersonálne vzťahy, inštitucionálne prostredie, zamestnanci. K upevňovaniu pozitívnej klímy v školách navrhuje praktický postup (Petlák 2006):

- Povedať a určiť rozumné nároky na správanie žiakov (hranice správania).
- Dodržiavať nároky na celý pedagogický kolektív – jednotne. Nejednotnosť vyvoláva pobúrenosť a labilitu študentov.
- Nároky sa predkladajú príjemne – ale zreteľne, stručne a jasne.
- Spoznať názory študentov – oblasť motivácie, práca v skupinách, vyučovanie a aktivity.
- Učiteľ ide vždy príkladom pre študentov učitelia dodržiavajú také správanie, aké požadujú od svojich študentov.

1.2 PRINCÍPY POZITÍVNEJ EDUKÁCIE

Z historických prameňov aj z odkazu nášho velikána učiteľa národov J. A. Komenského sú známe aj princípy ako základné požiadavky na vyučovací proces. Z didaktického hľadiská sú princípy edukácie aj dnes definované ak isté požiadavky, zásady, ktoré musí učiteľ vo svojom pôsobení na študentov rešpektovať a akceptovať. Z pohľadu pozitívne edukácie sú spracované princípy podľa Zelinu (2016):

- **zabezpečenie pozitívnej klímy** - škola a kultúra škola- rodinná a životná klím,
- **rešpektovanie pozitívnych hodnôt,**
- **pozitívne aplikovanie vedomostí v živote –** akcent na kvalitné vzdelanie,
- **stratégie podporujúce kritické, hodnotiace myslenie** a sebahodnotenie ,
- **tvorenie produktívnych interakcií .** vzťahy založené na empatii, akceptovaní,
- **motivovať k učeniu –** prostredníctvom zaujímavých úloh,
- **zdôrazňovať sebareflexiu, sebahodnotenie, sebakontrolu, sebriadenia študenta-** SPV, programy kultivácie charakteru,
- **emocionálne prežívať klímu v triede –** zisťovať ju a pozitívne merať, hodnotiť prežívanie , učiť vyjadrovať emócie a city – ovládať ich najmä v záťažových situáciách, komunikovať otvorene a kreatívne, sústrediť sa na racionálnu komunikáciu, komunikáciu citov, emócii a prežívania.

Z uvedených zásad – princípov je jasne, že treba rešpektovať princípy, ktoré pozitívne pôsobia v edukačnej realite a vedieť ich aj transformovať do každodenného života v zmysle hesla spojenie teórie s praxou. Zlepší to nielen duševné zdravie a spokojnosť so životom, zníži depresiu a úzkosť a zlepší ekonomický úspech a tvorivé myslenie – čo je aj zmyslom humanistického vyučovania. Hlavnou myšlienkou tejto pozitívnej edukácie je pozerať na edukáciu cez uspokojovanie potrieb učiaceho sa. Uplatňovanie prvkov a efektov pozitívnej psychológie v pedagogickej praxi podľa Zelinu (2018) ukazuje, že :

- sebadisciplína, vnútorná motivácia, ktorú zdôrazňuje pozitívna psychológia, je dvakrát lepším prediktorom výkonov, uplatnenia a úspechov v živote ako IQ a EQ,

- šťastní mladí ľudia v adolescencii, ako ukazujú longitudinálne výskumy, majú v dospelosti vyššie príjmy,
- angažovanosť a zmysluplnosť činností, ktoré akceptuje pozitívna psychológia sú najlepšou prevenciou proti depresiám,
- pozitívne prežívanie a zmysluplnosť bytia podporujú životnú spokojnosť a pozitívne pôsobí na učebný proces a to na kreatívne učenie.

Pozitívna edukácia pomáha študentom vybudovať si dôveru pri vzdelávaní, pri rozvíjaní intelektu a charakteru a rozvoji efektívnej stránky osobnosti. Pomáha uvedomiť si lepšie seba samého ako súčasť spoločenstva, podporuje intenzívny vzťah ku škole, školskému zariadeniu, zvyšuje školskú úspešnosť a kvalitu života v školskom prostredí i mimo neho.

Ak budem otrokmi digitálnych technológii a budeme hľadať útechu v technologických náhradách vzťahov, stratíme postupne sociálne zručnosti a naše sociálno-emocionálne správanie našej mládeže bude čím ďalej tým viac zasiahnuté depresiou, chaosom a nudou.

2. INTELEKTUÁLNA ODVAHA, ZBABELOSŤ A UNÁHLENOSŤ- KULTIVÁCIA CHARAKTERU ČLOVEKA 21. STOROČIA.

„Najvyšším princípom je konať „dobro a vyhýbať sa zlu“.

Keďže sa každý deň aj v podmienkach OS SR stretávame s rôznymi emóciami, ktoré ovplyvňujú naše konanie a rozhodovanie, to či dokážeme podľahnúť alebo ich korigovať určuje sila intelektuálnej odvahy – odvaha je vlastne cnosť, ktorá sa prejavuje ako vedomie potreby čeliť a spravodlivo riešiť myšlienky, ku ktorým máme silné negatívne emócie a relevantne argumenty s racionálnym zdôvodnením.

Intelektuálna odvaha stojí medzi dvoma neresťami - medzi nedostatkom, ktorý sa vyznačuje zbabelosť a medzi prebytkom, ktorý sa prejavuje ako unáhlenosť bez reflexii dopadu na vlastné konanie.

Intelektuálnu odvahu prejavujeme vtedy, keď sme ochotní utrpieť potenciálnu stravu alebo ujmu v záujme nejakého dobra keď súdime, že sa oplatí podstúpiť určite riziko (Intellectual Virtues Academy, 2022), Kosturková 2022 s.2).

Odborníci uvádzajú minimálne šesť druhov odváh (podľa Kosturkovej 2022,s.2):

- Fyzická odvaha – rozvoj fyzickej sily, odolnosti a uvedomelosti
- Sociálna odvaha – riziko spoločenských rozpakov, vylúčenia, neobľúbenosti, či odmietania
- Morálna odvaha- robiť správne vecí, najmä ak rizika zahŕňajú hanbu, odpor, alebo nesúhlas iných.
- Emociálna odvaha – otvára pocity celého spektra pozitívnych emócií s rizikom, že narazíme na tie negatívne (silno korešponduje so šťastím).
- Duchovná odvaha – keď zápasíme s otázkami o viere , zmysle života apod.

Niekedy sa môže stať, že odvaha na jednej strane sa ocitá v kontraste so zbabelosťou, ak sa človek nemá odvahu sa vyjadriť, alebo konať a na druhej strane jej kontrastom môže byť aj unáhlenosť. Ak chce človek prejaviť dne s intelektuálnu odvahu, odporúčame zvážiť najmä: všetky okolnosti, mať v danej vecí prehľad, neprijímať hotové informácie, ale kritický skúmať z viacerých hľadísk, názorov bez vlastných negatívnych emócii,.

Intelektuálna odvaha znamená byť skôr vnútorne motivovaný učiť sa, klásť otázky a hľadať spravodlivé odpovede (alebo riešenia). Takúto odvahu potrebujem tak v profesijnom ako aj v osobnom živte. Absencia intelektuálnej odvahy spôsobuje, že nemáme odvahu spochybniť presvedčenia, ktoré majú naši kolegovia, ale my s nimi nesúhlasíme. &nie sme schopní ani spochybniť etiku och rozhodnutí, správanie sa v prácu z morálneho hľadiska.

Absencia intelektuálnej odvahy je aj príčinou strachu z možného odmietnutia a súvisí s kognitívnou zrelosťou – čo je jedná z najdôležitejších dispozícií kriticky spravodlivého mysliteľa. Je to vlastne schopnosť postaviť sa voči myšlienkam, presvedčeniam, stanoviskám, ku ktorým máme silné negatívne emócie tak, že ich dokážeme spravodlivo posúdiť. Ak by sme žili bez emócii, tak by sme nevedeli mnohé vecí prežiť, niečo nepríjemne, neubezpečené a pod. Učia nás ktorým situáciám s vyhýbať a ktoré situácie vyhľadávať.

Opakom intelektuálnej odvahy je intelektuálna zbabelosť- strach z myšlienok, ktoré sa nezhodujú s myšlienkami konkrétneho človeka, Proti reakciou na intelektuálnu odvahu je často deštruktívna sila- zastrašovanie (strach je prvou formou intelektuálnej zbabelosti) osobnú odvahu treba zdokonaľovať vo vlastnom myslení a stávať s atak v živote rozumnejší. Hnev, strach a stres najčastejšie pociťujeme, keď myslíme, že nás niekto oklamal, zachoval sa nefér, cítime sa nedocenení apod.

2.1 STRATÉGIE ELIMINUJÚCE SILNÉ EMÓCIE

Zručnosti emocionálnej regulácie a zvládanie silných emócii sú dôležité interpersonálne zručnosti, vecí uvedené v hneve sa nedajú vziať späť. Častokrát aj rozhodnutie urobené v hneve nemajú veľa spoločného s racionálnym úsudkom. Preto je potrebné zvládať svoje emócie, a využívať vlastný potenciál racionálne a s odvahou. Odborníci z Univerzity z Virginie (UVA Healt 2022) uvádzajú tento konkrétny návod v programe pohody a múdrosti: uznajte svoj pocit, používajte pauzy, uzemnite sa, preskúmajte pocity vo svojom tele, myšlienky. Efektívne zvládanie silných emócii je vždy spojené s efektívnymi medziľudskými interakciami a facilitáciou cieľov. Je to vlastne adaptívna a dôležitá zručnosť pre každého človeka.

Psychológovia odporúčajú aj ďalšie stratégie, ktoré pomáhajú ľudom vyrovnať sa so silnými emóciami v zmysle odporúčaní: Ja to zvládnem, snažím sa zo všetkých síl, mám dobrý zmysel pre humor, dobré vecí hovoria samy za seba. Vedieť že je potrebné dodržiavať: dostatočnú dĺžku spania, pravidelne jesť, cvičiť a viesť zdravý životný štýl, vyhýbať sa látkam, ktoré menia náladu apod. „Druhých ľudí vieme zmeniť len málokedy, to je dokážeme zmeniť je náš postoj k situácii a druhému človeku“. (Neuschlová V, 2020).

Z uvedených zdrojov vyplýva, že v súčasnosti mnoho ľudí má potrebu s a vysporiadať sa s neetickými, nebezpečnými alebo diskriminačnými praktikami. Súvisí to najmä s etickou citlivosťou svedomím a skúsenosťami. Samozrejme, že idú do popredia: morálna integrita, zodpovednosť, čestnosť, odhodlanie, vytrvalosť a osobné rizoko.

Osobný profesijný rozvoj by mal byť aj v rámci kariérneho vzdelávania zameraný na morálnu odvahu, morálne hodnoty a etické princípy a neustále rozvíjať odvahu prostredníctvom vzdelávania, školení a praxe. V rámci stratégie CODE:
C / courade – odvaha byť morálnym,
O / obligations to honor- povinnosť ctiť si to, čo je správne urobiť,
D/ danger mangement/ - zvládanie hnevu- strachu (čo potrebujem ma zvládanie),
E/ expression and action) – vyjadrenie a konanie- aké kroky musím urobiť, aby som si zachoval integritu.(Kosturková, 2022 s. 5).

ZÁVER

Ak chceme prosperovať na pracovisku , ktoré je definované učiacou sa organizáciou a častými zmenami, je nevyhnutné sa neustále vzdelávať, mať ochotu skúšať nové vecí, produktívne bojovať a učiť sa aj pokusom a omylom. Samozrejme , že aj riešiť neznáme úlohy, hádanky, myslieť a prijímať chyby ako súčasť objavovania - to všetko je súčasť intelektuálnej kultúry. Najvyšším princípom je „konať dobro a vyhýbať sa zlu“. Naučiť sa byť integrálnou

a autonómnou osobnosťou v 21. storočí. To je výzva pre všetkých pedagógov a lektorov pôsobiacich v rezorte obrany.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BLAŠTÍKOVÁ, L.: 2018. Významné oblasti pozitívnéhjo klimatu školy v kontexte vybraných modelu. In: Lifelong Learning- celoživotné vzdelávaní, roč. 8, č.1. s.25-41. ISSN 1804-526X

VALJENTOVÁ, Z.: 2020. Pozitívna edukácia- paradigma súčasnej edukácie. Dubnica nad Váhom, Bakalárská práca Vysoká škola DTI, 64s

VALJENTOVÁ, Z.: 2020. Pozitívna edukácia a súčasná škola, Bratislava, DIDAKTIKA 3/2022, Wolters Kluver SR, s.r.o. EV 5869/19 ISSN 0338-2845, s.10-15

SELIGMAN, M.: 2014. Vzkvétaní. Brno, Jan Melvin publishing, 408 s. ISBN 788-08-727-0950

PETERSON, C. SELIGMAN, M.E.: 2004.Character strenghts and virtues. A handbook and clasisifications. Amerika. Psychological Association 888ptp. ISBN 978-0-19-57-16701-6

SELIGMAN, M. E.: 2012. Flourish: AVisionary New Understanding of Happiness and Well-being, 1. vydanie- dotlač, NewYork City: Simon and Schuster, 2012, 368s. ISBN 978-1-4391-9076-0

ZELINA, M. a kol.: 2016. Škola pre život v interdisciplinárnom kontexte. Brno:Tribun EU s.r.o. 284 s. ISBN 978-80-263-1062-4

ZELINA, M.: 2018. Psychoedukácia. Aplikovaná pedagogická psychológia. Dubnica nad Váhom: Vysoká škola DTI, 270 s. ISBN 978-80-89732-75-3

KANTOROVÁ, J.2015. Školní klima na školách poskytujúcioch strední vzdelávani s vyučným listem. Olomouc. Pedagogická fakulta, Univerzita Palackého.

PETLÁK, E. :2020. Motivácia v edukačnom procese. Bratislava: Wolters Kluwer, 104 s. ISBN 978-80-571-0150-5

PETLÁK, E.:2006. Klima školy aa klima triedy. Bratislava: IRIS, 119 s.ISBN 80-89018-97-1

KOSTURKOVÁ,M.: Intelektuálna odvaha, zbabelosť a unáhlenosť. Bratislava DIDAKTIKA 3/2022, Wolters Kluver SR, s.r.o. EV 5869/19 ISSN 0338-2845, s.2-5

NEUSCHLOVÁ, V.: 2020 Hnev a empatia - časté emócie v krízovom manažmente (online) 2020-04-03. Retrieved from: htps:// www. podnikajte.sk /manažment a stratégia/ empatia-emócie- krízový – manažment

doc. PhDr. Mária PETRUFOVÁ, PhD.
Katedra spoločenských vied a jazykov
AOS gen. M. R. Štefánika
03101 Liptovský Mikuláš

APLIKÁCIA KYBERNETICKEJ BEZPEČNOSTI VO VESMÍRNOM SEKTORE Z POHĽADU NATO

APLICATION OF CYBER SECURITY IN SPACE OF NATO'S PERSPECTIVE

Peter POLÁČEK

ABSTRACT

NATO as an organization is dependent on the proper functioning of information and communication technologies. Failure to do so can have adverse consequences. This is one of the reasons why the phenomenon of cyber security and the issue of protection of the cyber environment and critical infrastructure in space come to the fore. Space is a dynamic and rapidly evolving area, which is essential to the Alliance's deterrence and defence. In 2019, Allies adopted NATO's Space Policy and recognised space as a new operational domain, alongside air, land, sea and cyberspace. It will guide NATO's approach to space and ensure the right support to the Alliance's operations and missions in such areas as communications, navigation and intelligence. Through the use of satellites, Allies and NATO can respond to crises with greater speed, effectiveness and precision.

Key words : space, security, cyber attack, cyberspace

ÚVOD

Vesmírny priestor je dlhodobo využívaný na podporu pozemných vojenských a bezpečnostných zložiek. Využívanie vesmírnych technológii poskytlo nové možnosti velenia a riadenia vojenských síl kdekoľvek na svete. V súčasnosti sú vo vesmíre trvalo umiestnené satelity, ktoré okrem zhromažďovania spravodajských informácii slúžia okrem iného aj k navigácii, komunikácii, sledovaniu počasia, alebo k výskumu.

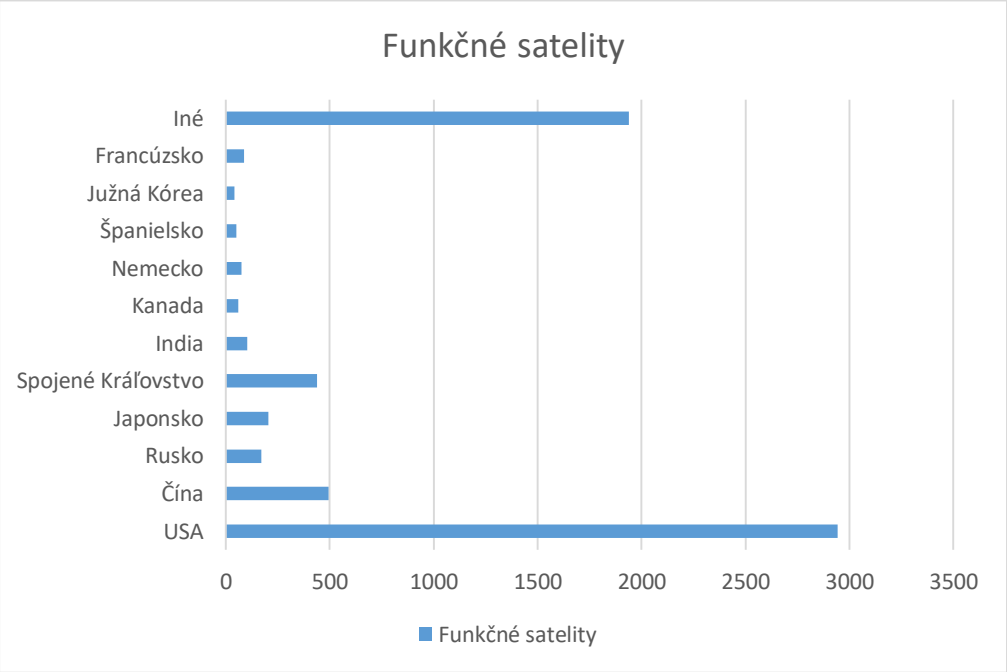
Aktivity NATO sú vo vesmíre zamerané na podporu pozemných, námorných a vzdušných operácií Aliancie v zmysle konceptu C4ISR (C2-Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). To zahŕňa využívanie technológií, vesmírnej infraštruktúry a väčšiu spoluprácu s civilným sektorom zameranú na národný záujem. Ide tak o schopnosti primárne určené pre informačnú dominanciu, orientáciu na bojisku a možnosti prijímania efektívnych a správnych rozhodnutí v reálnom čase (Lockheed Martin 2020). Bezpečnosť vesmírnych informačných systémov tak nadobúda veľký význam. V súčasnosti sa v tomto kontexte používa častejšie pojem kybernetická bezpečnosť.

Krajiny smerujúce do vesmíru musia počítať s antisatelitnými zbraňami vystrelenými zo Zeme a dokonca aj s perspektívou vesmírnych zbraní, ktorými môžu bojovať proti sebe a zároveň ohrozovať Zem z vesmíru.

Vojna vo vesmíre sa nelíši od vojny na mori kvôli stratégii a taktike konfliktu v týchto sférach ale preto, že sa líšia lietadlá od lodí ako a samozrejme tieto sa líšia od tankov a satelitov. Každá technológia formuje, definuje a vymedzuje nový druh vojny. Zvyšujúca sa prevádzka vo vesmíre tým pádom ovplyvňuje aj bezpečnosť, ktorá je spojená s ovládateľnosťou a kontrolou satelitov pred ohrozením z kolízie s inými satelitmi. Hoci je kybernetická bezpečnosť nepriamo spojená s tou vesmírnou, je táto technická záležitosť stále viac v súčasnosti akcentovaná v súvislosti s vesmírnymi systémami. Škodlivé rušenie totiž satelit nemusí zničiť (hoci k dočasnému aj trvalému poškodeniu dôjsť môže), obmedzí alebo vyradí jeho funkčnosť z prevádzky,

a teda možno povedať, že oproti antisatelitným zbraniam ide o jemnejšiu formu boja, a to platí dvojnásobne vďaka bežne používaniu výpočtových technológií. Pri kybernetických hrozbách voči satelitným systémom možno hovoriť o dvoch formách. Prvá pôsobí na satelity na obežnej dráhe a druhá potom na pozemné zariadenia (riadiace centrá a parabolické antény určené na príjem a vysielanie signálov medzi centrom a satelitom (NATO Science and Technology Organization 2020).

Vesmírne operácie NATO budú ovplyvňované širokou škálou technológií. Medzi najdôležitejšie bude patriť spoliehanie sa na vývoj umelej inteligencie, ktorá by uľahčila prijímanie predpokladaného nárastu informatívnych údajov z vesmíru. Medzi tieto technológie patrí zvýšené požívanie digitálnej reality (virtuálnej, zmiešanej atď.), vysokorýchlostný prenos dát vo vesmíre a z vesmíru na Zem a optická komunikácia (NATO Science and Technology Organization 2020).



Obrázok 1: Funkčné satelity na obežnej dráhe podľa jednotlivých krajín k 1. januáru 2022.
Zdroj: vlastný, upravené z USC Satellite Database (2022)

1 ZÁKLADNÉ TEORETICKÉ VÝCHODISKÁ

Vesmírny priestor

Z hľadiska ohraničenia sledovanej oblasti je potrebné vytýčiť rozdielnosť medzi vesmírnym priestorom a zemskou atmosférou. Definičný deliaci bod je takzvaná Kármánova línia, pomenovaná podľa maďarsko-amerického fyzika Theodora Kármána, ktorý ju dokázal zhruba určiť na 100 kilometrov nad hranicou morskej hladiny. V stručnosti, podľa vojenskej vesmírnej doktríny Veľkej Británie sa jedná o atmosférický bod, ktorý je pre bežné letectvo najvyšším dosiahnuteľným bodom. Naopak pre vesmírne plavidlo je to najnižší bod, pod ktorým je atmosféra príliš hustá na to, aby mohlo zotrvať na stabilnej orbite bez kontinuálneho ťahu svojho pohonu (MINISTRY OF DEFENCE.: The UK Military Space Primer. 2010. s. 1-2.)[1] .

[1] Bližšie pozri MINISTRY OF DEFENCE.: The UK Military Space Primer. 2010. s. 1-2.

Bezpečnosť

S pojmom bezpečnosť sa môžeme stretnúť vo viacerých vedných odboroch (spoločenskovedných, prírodovedných a technických), v ktorých má tento termín vždy svoj špecifický význam a charakter. V súčasnej legislatíve ani v odbornej literatúre neexistuje jednotná definícia či záväzný výklad pojmu bezpečnosť. Jednotlivý autori kladú dôraz na rôzne princípy, zásady a dimenzie. (PORADA, V. a kol., 2019, s. 51).

Vesmírna bezpečnosť

Vesmírna bezpečnosť je termín, ktorý nemá univerzálnu definíciu. Space Security Index definuje v 16. výročnej správe vesmírnu bezpečnosť ako bezpečný a udržateľný prístup k vesmíru a jeho využívanie a slobodu od hrozieb vychádzajúcich z priestoru pričom vychádza z vesmírnej zmluvy prijatej Výborom OSN v roku 1967[2] (SPACE SECURITY INDEX. *Executive Summary* 2019. [online]). Podľa tejto zmluvy by mal vesmír zostať voľne dostupný k mierovému využitiu pre všetkých aj v budúcnosti. Kľúčovým hľadiskom pri tomto prístupe k vesmírnej bezpečnosti nie sú záujmy konkrétnych národných alebo komerčných subjektov, ale bezpečnosť a udržateľnosť kozmického priestoru ako prostredia, ktoré môžu bezpečne a zodpovedne využívať všetci. Táto definícia zahŕňa udržateľnosť jedinečného vesmírneho prostredia, fyzickú a prevádzkovú integritu ľudských objektov vo vesmíre a ich pozemných staníc, ako aj bezpečnosť na Zemi pred hrozbami a prírodnými nebezpečenstvami vznikajúcich vo vesmíre.

Kybernetická bezpečnosť

Pri definovaní pojmu kybernetická bezpečnosť je potrebné si všimnúť rozdielnosť v terminológií. NATO vo svojich dokumentoch používa pojem kybernetická bezpečnosť, pričom Európska Únia preferuje skôr pojmy ako bezpečnosť sietí a informácií, informačná bezpečnosť. Kybernetickú bezpečnosť definujeme ako súhrn politík a nástrojov zabezpečujúcich spoľahlivosť a bezpečnosť prevádzky sietí a ochranu dát, teda zabezpečenie odolnosti komunikačných sietí pred prípadnými intervenciami zvonku, ale aj zvnútra. Ďalej je definovaná ako odbor výpočtovej techniky, resp. informačnej spoločnosti, ktorý sa presadil pri počítačoch ako aj sieťach (Cyber Security (Kybernetická bezpečnost) [online]). Kybernetická bezpečnosť sa líši od informačnej bezpečnosti prostredím, v ktorom sú dáta spracovávané a v ktorom sa odohrávajú, alebo môžu na nich odohrávať útoky (Porada V., 2019, s. 160). Jirásek, Novák a Požár definujú kybernetickú bezpečnosť ako „súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru“ (Jirásek, P., Novák L., Požár, J. 2015, s. 57). Ako uvádza Viktor Porada, že v spoločnom oznámení Európskemu Parlamentu a Rade (2017) sa zdôrazňuje:

- Kybernetická bezpečnosť (KB) je kriticky dôležitá pre našu prosperitu a bezpečnosť. Čím viac sa naše každodenné životy a ekonomiky stávajú závislejšie na digitálnych technológiách, tým viac sme vystavený kybernetickým hrozbám. Kybernetické bezpečnostné incidenty sa stále viac rôznia, a to z hľadiska toho, kto je za nich zodpovedný a čoho chce tým dosiahnuť. Nekalé činnosti v kybernetickom priestore ohrozujú nielen naše ekonomiky a presadzovanie jednotného digitálneho trhu, ale aj taktiež samotné fungovanie našich demokracií, našej slo-

[2] Bližšie pozri SPACE SECURITY INDEX. *Executive Summary* 2019. [online].

body a hodnôt. Naša budúca bezpečnosť závisí na transformácií našich schopností chrániť EÚ pred kybernetickými hrozbami: civilná infraštruktúra a vojenská kapacita sa opiera o bezpečné digitálne systémy.

- Riziká rastú exponenciálne. Štúdie ukazujú, že hospodársky dopad kyberkriminality sa od roku 2013 do roku 2019 zvýšil päťnásobne a bude sa ďalej zvyšovať.
- Kybernetické hrozby pochádzajú ako od neštátnych subjektov tak aj od štátnych: často ide o trestnú činnosť motivovanú ziskom, dôvody môžu byť však aj politické ako aj strategické.
- Štátne subjekty dosahujú stále vo väčšej miere svojich geopolitických cieľov nielen prostredníctvom tradičných nástrojov, akým je vojenská sila, ale taktiež pomocou menej nápadných kybernetických nástrojov ako aj zasahovaním do vnútorných demokratických procesov. V súčasnej dobe sa všeobecne pripisuje využívanie kybernetického priestoru ako oblasť vedenia vojny a to buď samostatne, alebo v rámci hybridného prístupu (Porada V., 2019, s. 160-161).

Kybernetickú ako aj informačnú bezpečnosť charakterizuje tzv. CIA triáda (CIA triad), ktorá obsahuje tri hlavné princípy. Prvým je dôvernosť (Confidentiality), ktorý vyjadruje snahu zaistiť ochranu prenášaných či uschovaných informácií pred prípadným odpočúvaním a čítaním. Cieľom druhého princípu celistvosti (Availability) je chrániť informácie a systémové funkcie pred protiprávnou manipuláciou a reguláciou. Dostupnosť dát (Integrity) je tretím princípom na základe ktorého by mali byť všetky informácie a služby dostupné vždy, keď je to pre oprávneného užívateľa potrebné (ČERMÁK, M., 2009, [online]).

Obrázok 2: CIA Triáda
Zdroj: ČERMÁK, M. Informační bezpečnost. In Clever Smart. 2009

Na kybernetickú bezpečnosť môžeme nahliadať z viacerých aspektov. Z informačného hľadiska sa jedná o IT zabezpečenie s dôrazom na zabezpečenie internetu. Metódy sú teda zamerané na boj proti hrozbám dátovej (vesmírnej) infraštruktúry technickými prostriedkami. Medzi hlavné hrozby zaraďujeme zlyhanie systému, nesprávne programovanie alebo zlyhanie ľudského faktora. V rámci kybernetickej bezpečnosti sú na jednej strane dôležité prostriedky zabezpečujúce technickú stránku, avšak na druhej stránke je potrebné vyzdvihnúť spoločenskú

stránku. V porovnaní s klasickou bezpečnosťou na štátnej úrovni, je v rámci kybernetickej bezpečnosti nutné koordinovať bezpečnostné aktivity so súkromným a akademickým sektorom, ale i s výchovou jednotlivých užívateľov. Špecifikom zabezpečenia kybernetickej bezpečnosti je i nevyhnutnosť koordinovať aktivity na medzinárodnej úrovni, nielen na úrovni jednotlivých štátov. Cieľom jednotlivých štátov by malo byť prijatie strategických bezpečnostných nástrojov adekvátnych ku kybernetickým hrozbám a v neposlednom rade vytvorenie a prijatie legislatívnej úpravy danej problematiky.

Kybernetický priestor

S kybernetickou bezpečnosťou sa nespochybniteľne spája pojem kybernetického priestoru, ktorý je jej predmetom ochrany. V príspevku chápeme vesmír ako časť kybernetického priestoru.

Podľa vymedzení základných pojmov v zmysle § 3 písm. c) zákona číslo 69/2018 Z.z. o kybernetickej bezpečnosti sa pod pojmom kybernetický priestor uvádza, že na účely tohto zákona rozumie:

„ Kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.“ (§ 3 písm. c) zákona číslo 69/2018 Z.z. o kybernetickej bezpečnosti).

Výkladový slovník kybernetickej bezpečnosti definuje „kybernetický priestor ako digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorené informačnými systémami a službami a sieťami elektronických komunikácií” (Jirásek – Novák - Požár, 2015, s. 59). Volner hovorí o online prostredí, kde sa eliminuje vzdialenosť a čas. V tomto priestore budú dominovať najmä informačná, kybernetická a psychologická vojna, ktoré budú neoddeliteľné. Kybernetické zbrane tak môžu predstavovať informácie, elektronické a počítačové nástroje a ďalšie. (Volner, 2007).

Kybernetický priestor zásadne zmenil náš spôsob života, poskytujúc miliardám ľudí po celom svete okamžitý prístup k informáciám, ku komunikácii, obchodným príležitostiam. Je novou hranicou, plnou príležitostí na zlepšenie bezpečnosti a prosperity 21. storočí. Je bojiskom budúcnosti, v ktorom sa nepriatelia budú snažiť spôsobiť škody štátu, ekonomike a občanom. hrozieb. Mnoho jednotlivcov považuje kybernetický priestor za samostatný vojenský priestor.

Na rozdiel od iných oblastí, ktoré sú do značnej miery charakterizované prirodzenými fyzikálnymi vlastnosťami, kybernetická oblasť je definovaná predovšetkým jeho nefyzikálnymi vlastnosťami. Limity kyberpriestoru sú elektromagnetické spektrum, na ktorom je pri súčasnej konfigurácii závislý a rýchlosť svetla, ktorá určuje hornú hranicu rýchlosti kyberkomunikácie.

Kybernetický priestor je systémom zloženým z troch vrstiev. Prvú vrstvu, fyzickú, tvoria geografické zložky, v rámci ktorých sa jedná o rozloženie jednotlivých prvkov siete. Do tejto vrstvy zaraďujeme hardware, routery, servery, elektromagnetické spektrum a mnohé ďalšie zariadenia tvoriace fyzickú časť kyberpriestoru. Logická vrstva sa skladá z logických spojení medzi jednotlivými uzlami počítačov pripojených k sieti. Uzol je chápaný ako zariadenie s IP (Internet Protocol) adresou. Obsahom sociálnej vrstvy sú kognitívne a ľudské faktory, ktoré reprezentuje persona a kybernetická persona. Z uvedeného vyplýva, že kybernetický priestor môžeme chápať ako sféru prepojenú s fyzickým svetom, logickou vrstvou a ľudským vnímaním.

K vymedzeniu pojmu kybernetického priestoru prispieva fakt, že kybernetický priestor sa neustále rozširuje a zasahuje do viacerých oblastí spoločnosti. Nie je geograficky ohraničený a vzdialenosť v takomto priestore nie je obmedzená a zanedbateľná. Myslíme si, že najvážnejším problémom kybernetickej bezpečnosti, resp. kybernetického priestoru je otázka suverenity.

Operácia uskutočnená v jednom štáte môže mať okamžité následky kdekoľvek na svete, pretože kybernetický priestor nemá presne vymedzené hranice. K zvýšeniu bezpečnosti systémov je dôležitý každý jeden prvok, zároveň však tieto prvky môžu byť eventuálnymi prekážkami v efektívnom riadení aktivít v kybernetickom priestore. Vzhľadom na určité vynaložené náklady na tieto elementy si dovolíme tvrdiť, že ekonomický aspekt zabezpečenia kybernetického priestoru bude vždy prekážkou v odstránení niektorých kybernetických hrozieb.

Kybernetická obrana

Kybernetická obrana je súčasťou obrany NATO od roku 2002, kedy bol na samite v Prahe prijatý program Cyber Defence. Odpoveďou na závažnosť kybernetických hrozieb bolo zriadenie Centra kybernetickej obrany v hlavnom meste Estónska Talline a zostavenie oficiálnej stratégie kybernetickej obrany v roku 2008. Následne v roku 2010 vznikli dve centrá NATO s cieľom posilnenia kybernetickej obrany Centrum Defence Management Authority a centrum excelentnosti NATO Cyber Defence of Excellence.

Pre zvýšenie kybernetickej bezpečnosti a posilnenia obrany proti kybernetickým útokom bola na pôde NATO prijatá nová politika, ktorá stanovila, že obrana proti kybernetickým útokom je súčasťou kľúčových úloh kolektívnej obrany NATO. Hlavnou prioritou novej politiky NATO je ochrana komunikačných systémov, ktoré vlastní alebo prevádzkuje NATO. Hlavnými aktivitami v oblasti kybernetickej bezpečnosti sú:

1. Presadzovanie politiky kybernetickej obrany NATO;
2. Asistencia jednotlivým spojeneckým krajinám;
3. Zvyšovanie kapacity kybernetickej obrany NATO;
4. Spolupráca s partnermi;
5. Spolupráca s priemyslom (Hromada M. 2015, [online])

Varšavský samit NATO, ktorý sa konal 8.-9. júla v roku 2016 privítal hlavy štátov a vlád členských krajín. Konal sa takmer dva roky po konferencii vo Walese na ktorom sa rozhodlo, že medzinárodné právo sa vzťahuje na kybernetický priestor a kybernetická obrana je súčasťou základnej úlohy kolektívnej obrany NATO. Kybernetickou obranou sa v Communiqué zaoberajú články 71 a72. V týchto bodoch reprezentácie štátov a vlád znovu potvrdzujú obranný mandát NATO ohľadne úloh kolektívnej obrany v kybernetickom priestore. Teraz však už kybernetický priestor vymedzujú ako oblasť operácií. Kybernetický priestor v tomto poňatí chápeme ako novú dimenziu v ktorej sa NATO musí brániť tak efektívne ako vo vzduchu, na zemi a na mori (Warsaw Summit Communiqué, 2016 [online]). Communiqué sa následne odvoláva na dokument schválený na samite, ktorým je Cyber Defence Pledge (ďalej ako Sľub kybernetickej obrany). Sľub kybernetickej obrany je dokument, v ktorom sa uvádza, že členské krajiny zabezpečia, aby sa udržal krok s rýchlo sa vyvíjajúcou scénou kybernetických hrozieb (Cyber Defence Pledge, 2016, [online]).

Výrazným posunom vo vnímaní problematiky kybernetickej bezpečnosti bolo prijatie novej strategickej koncepcie NATO- Strategic Concept NATO 2022, ktorá bola schválená 29.6.2022 v Madride. Na rozdiel od poslednej koncepcie prijatej v Lisabone v roku 2010 došlo k zásadným zmenám v definovaní bezpečnostných výziev a hrozieb pre Alianciu, kde sa uvádza:

- Strategickí konkurenti a potenciálni protivníci investujú do technológií, ktoré by mohli obmedziť náš prístup a aktivity vo vesmíre, degradovať naše vesmírne spôsobilosti. Cielia sa na našu civilnú a vojenskú infraštruktúru, narúšajú našu obranu a bezpečnosť.
- Hoci je NATO obrannou alianciou, nikto by nemal pochybovať o našej sile a odhodlaní brániť každý centimeter spojeneckého územia, zachovávať nezávislosť a územnú suverenitu všetkých spojencov a zvíťaziť nad akýmkoľvek agresorom.

V strategickom prostredí konkurencie budeme zvyšovať naše globálne povedomie na odstrašenie a obranu vo všetkých doménach a smeroch.

- Kľúčom k bezpečnému a neobmedzenému prístupu do vesmíru a kybernetického priestoru je účinná obrana a odstrašovanie. Zvýšime našu schopnosť efektívne pôsobiť vo vesmíre a kybernetickom priestore prevenciou, detekciou a bojom proti celému spektru hrozieb pomocou všetkých dostupných nástrojov. Jeden alebo kumulatívny súbor škodlivých kybernetických aktivít, alebo nepriateľské operácie z alebo vo vesmíre môžu dosiahnuť úroveň ozbrojeného útoku a mohli by viesť k odvolaniu sa na článok 5 Severoatlantickej zmluvy. Uznávame uplatniteľnosť medzinárodného práva a budeme podporovať zodpovedné správanie sa vo vesmíre a kybernetickom priestore. Zvýšime tiež odolnosť vesmírnych a kybernetických spôsobilostí, od ktorých je naša kolektívna obrana a bezpečnosť závislá (Strategic Concept NATO 2022, 2022, [online]).

Veľká pozornosť sa venuje aj spolupráci NATO a EÚ v týchto záležitostiach. Zmluvné strany podpísali spoločné vyhlásenie, v ktorom sa kybernetická bezpečnosť a kybernetická obrana výslovne uvádzajú ako jej hlavné témy. Dňa 10. februára 2016 bola podpísaná technická dohoda, ktorá má poskytnúť rámec pre výmenu informácií a zdieľanie osvedčených postupov medzi tímami NATO Computer Incident Response Capability (ďalej ako NCIRC) a Computer Emergency Response Team for the European Union (ďalej ako CERT-EÚ). Technická dohoda je konkrétnym príkladom spolupráce NATO a EÚ na posilnení spoločnej bezpečnosti. Ide tiež o najnovší príklad dlhodobej spolupráce v oblasti kybernetickej obrany medzi týmito dvoma organizáciami. Zamestnanci kybernetickej obrany z Európskej únie sa okrem toho už niekoľko rokov zúčastňujú každoročného cvičenia kybernetickej obrany NATO Cyber Coalition (NATO and the European Union enhance cyber defence cooperation, 2016 [online]).

2 KYBERNETICKÉ HROZBY

V súčasnosti sa do popredia dostáva čoraz viac problematika kybernetických hrozieb. Za realizáciu kybernetickej hrozby môžeme považovať prevedenie kybernetického útoku. Podľa malého výkladového slovníka sa významom kybernetická hrozba označuje to, ak môžeme očakávať určitú hrozbu v rámci kybernetického priestoru (aktívam). To môžeme chápať ako hrozbu, ktorá bude realizovaná kybernetickými prostriedkami v kybernetickom prostredí.

Pojem kybernetické ohrozenie znamená nebezpečenstvo pred konkrétnou skupinou, alebo podsystémom v rámci celého kybernetického priestoru (Odbor riadenia kybernetickej a informačnej bezpečnosti, Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník, 2021, s. 29 [online]).

Práve kritická vesmírna infraštruktúra je v prípade kybernetických hrozieb jedna z najviac ohrozených oblastí. Všetky jej zložky sú závislé na informačnej infraštruktúre pri správe informácií, komunikácií a kontrolných funkciách. Kombinácia počítačov a komunikačných systémov dnes slúžia ako základná infraštruktúra pre vesmírne spôsobilosti a sú aj hlavnou zložkou vesmírneho bezpečnostného prostredia. Ako príklad môžeme použiť Spojené štáty americké, jeden z najvyspelejších štátov sveta - len samotné Ministerstvo obrany USA využíva 15 000 sietí a sedem miliónov kusov výpočtovej techniky, ktoré musia byť patrične zabezpečené a pravidelne kontrolované. Podľa amerického ministra obrany sú Spojené štáty americké pravidelne vystavované hrozbe kybernetického útoku od viac ako stovky zahraničných tajných služieb (Murphy, T., 2010. Security Challenges in the 21 st).

Špecifikom bezpečnostných hrozieb je aj skutočnosť, že ich vznik môže zapríčiniť nielen vedomé konanie, ale aj systémová chyba. Kybernetické hrozby často vyplývajú z nedostatkov, takzvaných zraniteľností, ktoré vo väčšine prípadov vznikajú neúmyselne už pri samotnom

vývoji bežne používaného softvéru alebo pri zabezpečovaní kritickej infraštruktúry. Zraniteľnosť v systéme môže byť využitá potenciálnym útočníkom. Ideálny stav, teda existencia systémov a softvérov bez využiteľných zraniteľností, je v súčasnosti prakticky nedosiahnuteľná (Kačmár, 2016).

Kybernetické bezpečnostné hrozby sú mimoriadne rôznorodé. Ciele útokov sa nenachádzajú len v štátnom aparáte a vojenskej sfére, ale aj v ekonomickom, environmentálnom a spoločenskom sektore. Kybernetická bezpečnosť vo vesmírnom priestore má jednoznačné vojenské implikácie a najmodernejšie technológie sú využívané práve ozbrojenými silami NATO, ktoré sú na vesmírnych informačných a komunikačných technológiách závislé. Okrem priamych vojenských bezpečnostných hrozieb, ktoré vyplývajú z možnosti, že vesmírne spôsobilosti, prípadne utajené informácie by sa dostali pod kontrolu nepriateľa, môžeme vymedziť aj nepriame a nevojenské kybernetické bezpečnostné hrozby. Vo všeobecnosti kybernetické hrozby môžeme rozdeliť do štyroch domén:

- štátne a štátmi sponzorované útoky,
- ideologický a politický extrémizmus,
- organizovaný zločin,
- individuálny zločin.

Jednotlivé domény a ich obsah sa navzájom prelínajú. Napríklad hacking môže byť individuálnym zločinom a neorganizovanou aktivitou, no jeho využitie je časté aj v iných doménach a s oveľa väčšími následkami, ako pri útokoch individuálnych hackerov. Najväčšiu pozornosť si získavajú útoky realizované štátnymi aktérmi, prípadne inými aktérmi s podporou štátov, a to najmä preto, že v prípade preukázateľnosti pôvodcu útokov majú najväčší potenciál vyvolať konflikt aj vo vesmírnej sfére.

Kybernetické hrozby vo vesmírnom priestore sú omnoho bezprostrednejšie ako tradičné vojenské hrozby. Sú mimoriadne sofistikované, a preto sa aj útočník ťažko stopuje. Pri väčšine kybernetických útokov môžeme len predpokladať, kto bol skutočným vinníkom a len veľmi zložito to vieme dokázať (Kačmár, 2016).

2.1 KYBERNETICKÝ ÚTOK A KYBERNETICKÁ ŠPIONÁŽ

Vzhľadom na neustále rastúcu závislosť vojenských spôsobilostí NATO na vesmírnom priestore sa do popredia čím ďalej, tým viac, dostáva oblasť kybernetickej bezpečnosti. V súčasnosti sú vo vesmíre trvalo umiestnené satelity, ktoré okrem zhromažďovania spravodajských informácii slúžia okrem iného aj k navigácii, komunikácii, sledovaniu počasia, alebo k výskumu. Hoci je kybernetická bezpečnosť nepriamo spojená s tou vesmírnou, je táto technická záležitosť stále viac v súčasnosti akcentovaná v súvislosti s vesmírnymi systémami. Škodlivé rušenie totiž satelit nemusí zničiť (hoci k dočasnému aj trvalému poškodeniu dôjsť môže.), obmedzí alebo vyradí jeho funkčnosť z prevádzky, a teda možno povedať, že oproti antisatelitným zbraniam ide o jemnejšiu formu boja, a to platí dvojnásobne vďaka bežne používaniu výpočtových technológií.

Pri kybernetických hrozbách možno voči satelitným systémom možno hovoriť o dvoch formách. Prvá pôsobí na satelity na obežnej dráhe a druhá potom na pozemné zariadenia (riadiace centrá a parabolické antény určené na príjem a vysielanie signálov medzi centrom a satelitom.

Vesmírne operácie NATO budú ovplyvňované širokou škálou technológií. Medzi najdôležitejšie bude patriť spoliehanie sa na vývoj umelej inteligencie, ktorá by uľahčila prijímanie predpokladaného nárastu informatívnych údajov z vesmíru. Medzi tieto technológie patrí zvýšené požívanie digitálnej reality (virtuálnej, zmiešanej atď.), vysokorýchlostný prenos dát vo vesmíre a z vesmíru na Zem, optická komunikácia**.** Tieto skutočnosti však so sebou prinášajú i negatívnu stránku, a to nárast kybernetických útokov.

Kybernetický útok je elektronický útok na systém podniku alebo jednotlivca, s cieľom narušiť, ukradnúť alebo poškodiť aktíva, pričom tieto aktíva môžu byť digitálne, napríklad údaje, informácie alebo užívateľský účet, ďalej digitálne služby, fyzické aktívum s kybernetickou zložkou. Jednou z úloh kybernetickej bezpečnosti je určitým spôsobom chrániť ich pred takýmto útokom, pretože jeho snahou je ohroziť integritu, dostupnosť digitálnych aktív alebo dôvernosť, ktorá zaisťuje, že dáta a informácie sú k dispozícii len oprávneným osobám. Môžu mať mnoho foriem a zahŕňať i aktíva dôležité pre udržanie pozície podniku na trhu. Jirásek, Novák, Požár charakterizujú kybernetický útok ako *„útok na IT infraštruktúru za účelom spôsobiť poškodenie a získať citlivé či strategicky dôležité informácie. Používa sa najčastejšie v kontexte politicky alebo vojensky motivovaných útokoch*".(Jirásek – Novák – Požár, 2015, s. 59). Z uvedených definícií vyplýva, že kybernetický útok môže byť spáchaný štátom alebo neštátnym aktérom, a má za následok nefunkčnosť systémov, špionážne aktivity alebo aktivity motivované získaním, resp. krádežou dát. Hlavnými črtami kybernetického útoku je anonymita útočníka, obtiažnosť určiť hlavný cieľ útoku a vysoká rýchlosť vedenia takéhoto útoku.

Jedným z najdiskutovanejších fenoménov spojených s kybernetickou bezpečnosťou je pojem kybernetická vojna. *„Hlavným cieľom kybernetickej vojny je narušiť komunikáciu nepriateľa."* (Volner, 2007, s. 270). Kybernetická vojna je politika rozšírená o opatrenia prijaté v kybernetickom priestore zo strany štátnych alebo neštátnych aktérov, ktoré buď predstavujú vážnu hrozbu pre bezpečnosť NATO a jeho spojencov, alebo sú vykonávané v reakcii na vnímané hrozby proti bezpečnosti národa.

Kybernetická špionáž je pokusom o preniknutie do počítačových sietí alebo systému za účelom získať citlivé alebo chránené informácie. Úlohou nie je dosiahnutie cieľa, ale zhromaždenie informácií, ktoré by mohli byť použité na konkrétnejšie nástroje a kroky.

Podľa Výkladového slovníka kybernetickej bezpečnosti je kybernetická špionáž *„získavanie strategicky citlivých či strategicky dôležitých informácií od jednotlivcov alebo organizácií za využitia prostriedkov IT. Používa sa najčastejšie v kontexte získavania politickej, ekonomickej alebo vojenskej prevahy"* (Jirásek – Novák - Požár, 2015, s. 70).

Jej cieľom je získanie prístupu k duševnému vlastníctvu a technologickým inováciám nadnárodných spoločností, ale aj štátnych inštitúcií. Kybernetickú špionáž však nevykonávajú len organizované skupiny zamerané na finančný zisk, ale aj štáty, ktoré sa takýmto spôsobom snažia získať utajené informácie, zväčša vojenského charakteru, iných štátov (Kačmár, 2016).

Aktivity kybernetickej špionáže sú oveľa viac presvedčivejšie ako aktivity v rámci kybernetickej vojny.

ZÁVER

NATO ako organizácia je závislá na správnom fungovaní informačných a komunikačných technológií. Ich znefunkčnenie môže mať neblahé dôsledky. I preto sa do popredia dostáva fenomén kybernetickej bezpečnosti a otázka ochrany kybernetického prostredia a kritickej infraštruktúry vo vesmíre. Význam bezpečnosti kybernetického priestoru nemožno podceňovať. Kybernetická bezpečnosť sa stala predmetom národných a medzinárodných politík, keďže nelegálne operácie v rámci kybernetického priestoru môžu spôsobiť ohrozenie národnej bezpečnosti, obrany, slobody, suverenity a nezávislosti či všetkých dôležitých činností štátu. V dôsledku toho zohráva významnú úlohu v konfliktoch v 21. storočí. Vznikajúce kybernetické hrozby, kybernetický útok, kybernetická vojna, kybernetický terorizmus a kybernetická špionáž, predstavujú ohrozenie ako pre kybernetickú bezpečnosť, tak aj pre národnú a medzinárodnú bezpečnosť. Uvedené hrozby sú namierené proti jednotlivcom, súkromným subjektom, vládnym zložkám alebo proti kritickej infraštruktúre štátov a organizácií.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

Cyber Defence Pledge, 2016. [online]. Dostupné na internete: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

CYBER SECURITY (Kybernetická bezpečnost). In *CyberSecurity.cz : Kybernetická bezpečnost.* Dostupné na internete: https://www.cybersecurity.cz/basic.html

ČERMÁK, M. 2009. *Informační bezpeč*nost. In *Clever Smart*. [online]. Dostupné na internete: http://www.cleverandsmart.cz/informacni bezpecnost/

DUNN, M. 2005. *A comparative analysis of cybersecurity initiatives worldwide.* [online]. Dostupné na internete: https://www.itu.int/osg/spu/cybersecurity.com

ENISA. 2011. *CERT-E.*[online]. Dostupné na internete : https://www.enisa.europa.eu/

HROMADA M. a kol.2015. *Kybernetická Bezpečnosť teórie a praxe*, 2015. [online]. Dostupné na internete: https://www.researchgate.net/publication/299489155_Cyber_Security_Theory_and_Practice

JIRÁSEK, P., NOVÁK L., POŽÁR, J. 2015. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie České republiky, 2015. 240 s. ISBN 978-80-7251-436-6.

KAČMÁR R. 2016. *Kybernetická bezpečnosť,*2016. [online]. Dostupné na internete: https://slovaksecurity.org/wp-content/uploads/2016/10/Kyberneticka-bezpecnost_SSPI.pdf

LOCKHEED MARTIN. 2020. *C4ISR Is the Foundation of Every Mission*. [online]. Dostupné na internete: https://www.lockheedmartin.com/en-us/capabilities/c4isr.html

MINISTRY OF DEFENSE. 2010. *The UK Miltary Space Primer.* United Kingdom 2010. [online]. Dostupné na internete: http://www.mod.uk

MURPHY, T. 2010. *Security Challenges in the 21 st Century Global Commons,* [online]. Dostupné na internete: http://files.redsafeworld.net/2000009465458a54d26/Global%20Commons.pdf

MIRRI. Odbor riadenia KIB. 2021. *Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník.*[online]. Dostupné na internete: https://www.mirri.gov.sk/wp-content/uploads/2021/06/KB-K1_2_3-Uvod-do-KIB_slovnik_ver1.0.pdf

NATO, 2016, *NATO and the European Union enhance cyber defence cooperation*,[online]. Dostupné na internete: https://www.nato.int/cps/en/natohq/news_127836.htm

NATO Science and Technology Organization 2020, *Science and Technology trends 2020-2040.* [online]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO, 2018, *NCI Agency,* [online]. Dostupné na internete: https://www.ncia.nato.int/what-we-do.html

NATO, 2016, *Warsaw Summit Communiqué*, [online]: Dostupné na internete: https://www.nato.int/cps/su/natohq/official_texts_133169.htm

NATO, 2022*, STRATEGIC CONCEPT NATO 2022*, [online]. Dostupné na internete: https://www.nato.int/strategic-concept/

PORADA V. a kolektív 2019.: *Bezpečnostní vědy*. Plzeň, Aleš Čeněk, s.r.o. 2019, 780 s. ISBN 978-80-7380-758-0.

SPACE SECURITY INDEX. 2019, *Executive Summary* 2019. [online]. ISBN: 978-1-927802-26- 7, Dostupné z: http://spacesecurityindex.org/ssi_editions/space-security-2019/

VOLNER, Š. 2007. *Nová teória bezpečnosti.* Zvolen: Bratia Sabovci, s.r.o., 2007. 296 s., ISBN 978-80-89241-12-5.

Zákon č. 69/2018 Z. z. *o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*

Ing. Peter POLÁČEK
Muškátová 15, Senec, 90301
E-mail : polacek.pepo@gmail.com

ZÁVAŽNOSŤ GLOBÁLNYCH ZDRAVOTNÝCH HROZIEB

THE IMPORTANCE OF GLOBAL HEALTH THREATS

Michaela ŠIMONOVÁ

ABSTRACT

Both individuals and society perceive life and health as the highest priority. Global health threats represent an unforeseen and uncontrolled threat to public health. The response to a health threat should include the detection and identification of the threat and then the targeted establishment of early warning channels through procedures that health authorities can use to exchange information.

Keywords: Health, threat, security threat, European Union.

ÚVOD

Ochrana života a zdravia je najvyššou prioritou každého jednotlivca, ale aj spoločnosti. Skvalitňovaním a rozšírením možnosti poskytovania zdravotnej starostlivosti došlo k zníženiu šírenia infekčných ochorení, avšak z dôvodu vysokej mobility ľudí stúpa riziko ohrozenia zdravia. Vzhľadom na uvedené je nutné zo strany štátov monitorovať zdroje nákazy a reagovať na jej prípadné šírenie.

Motiváciou pri písaní práce je poukázať na závažnosť globálnych zdravotných problémov v kontexte prítomných bezpečnostných hrozieb, a to za účelom začatia verejného dialógu a poukázania na dôležitosť spolupráce, monitorovania a výmeny informácií. Za hlavný cieľ sme si preto stanovili zanalyzovať prejavy a riziká globálnych zdravotných hrozieb a stav legislatívneho prostredia, inštitucionálneho zabezpečenia a aktivít na národnej úrovni a v rámci Európskej únie, ako aj poukázanie na dôležitosť venovania sa tejto problematike.

1 DEFINOVANIE ZÁKLADNYCH POJMOV V KONTEXTE HODNOTENIA GLOBÁLNYCH ZDRAVOTNÝCH HROZIEB

Definovanie pojmov je nástrojom, pomocou ktorého je možné konkrétny problém skúmať. Podľa K. Kampovej a K. Hollej *„význam definovania základných prvkov systému bezpečnosti je v poznaní ich vzťahov a identifikovaní možných nedostatkov a následnom určení prostriedkov na zaistenie požadovanej bezpečnosti. Bez dôkladného poznania systému nie je možné zaručiť jeho správne fungovanie a teda ani požadovanú úroveň bezpečnosti"* (Kampová a Hollá, 2013, s. 9).

„Bezpečnosť vo všeobecnosti predstavuje stav vedomia človeka, v ktorom sa necíti byť ohrozený, žije bez ohrozenia, nemá strach o seba ani o iných, je to istota do budúcnosti, absencia ohrozenia zdravia, straty majetku, psychický stav umožňujúci realizáciu životných cieľov a zámerov, a v neposlednom rade bezpečnosť predstavuje aj ustanovenie orgánov a inštitúcií, ktoré svojou činnosťou garantujú občanovi stav istoty a bezpečnosti" (Hofreiter a Brytusová, 2016, s. 17).

Bezpečnosť nie je možné skúmať bez toho, aby sme poznali aké hrozí nebezpečenstvo. Podľa V. Poradu je nebezpečenstvo pojem, ktorý označuje možnosť, že akýkoľvek činiteľ môže spôsobiť negatívny jav, ktorý môže následne viesť k negatívnemu vplyvu. Pojem nebezpečenstvo predstavuje vlastnosť objektu spôsobiť neočakávaný negatívny jav, ohrozenie referenčného objektu (Porada a kol., 2019).

Hrozba predstavuje blízkosť niečoho nepríjemného prípadne nebezpečného, čomu je vystavený človek a prostredie, v ktorom žije (Porada a kol., 2019). Š. Volner definuje hrozby ako *„javy a procesy ekonomického, politického,* ***sociálneho****, vojenského, geopolitického, ekologického, vedecko-technického, informačného, morálno-duchovného charakteru na najrôznejšej úrovni spoločenského života (od individuálnej až po globálnu), ktoré priamo* ***negatívne pôsobia na prírodu a spoločnosť, ohrozujú ich existenciu, fungovanie a rozvoj****"* (Volner, 2005, s. 119).

Potreba bezpečnosti nastupuje ihneď po potrebe potravy. Bezpečnosť spoločnosti stojí na základoch, ktoré sú spojené s človekom od jeho vzniku. Od potreby bezpečia jedinca sú odvodené potreby bezpečnosti – bezpečnosť sociálnych entít (rodina) až po bezpečnosť štátu a v dnešnej dobe celej ľudskej civilizácie. Bezpečnosť človeka má biologickú (zdravotnú), psychickú a sociálnu dimenziu a bezpečnostné hrozby a riziká existujú vo všetkých týchto dimenziách. Bezpečnosť človeka je vzťahovaná k životu a k jeho kvalite vo všetkých dimenziách. Hrozby a riziká voči bezpečnosti človeka existujú vo všetkých rovinách a človek je nimi diferencovane vystavený, diferencovane tieto hrozby vníma a diferencovane na ne reaguje. Zdrojom bezpečnosti a bezpečnostných hrozieb pre človeka je on sám, jeho rodina, jeho spoločnosť a vyššie civilizačné celky. V tomto poradí je schopný hrozby reflektovať a ovplyvniť (Porada a kol., 2019).

Každý jednotlivec aj spoločnosť vníma život a zdravie za najvyššiu prioritu. Význam **ľudskej bezpečnosti** narastá s rozvojom globalizácie. Ľudská bezpečnosť predstavuje národnú bezpečnosť - do centra pozornosti sa dostáva človek ako objekt ochrany a jeho osobné vnímanie hrozieb. Koncepcia ľudskej bezpečnosti v sebe zahŕňa ochranu človeka a všetkých jeho záujmov (Kampová a Hollá, 2013). Občania vnímajú bezpečnosť najmä ako stav vedomia, v ktorom sa necítia byť ohrození, život bez ohrozenia, stav bez strachu o seba či iných, **absenciu ohrozenia zdravia**, stratu majetku či života (Porada, a kol., 2000).

Zoznam hrozieb, ktoré ovplyvňujú ľudskú bezpečnosť je široký, ale väčšinu z nich je možné identifikovať v nasledovných kategóriách: ekonomická bezpečnosť, potravinová bezpečnosť, **bezpečnosť zdravia**, environmentálna bezpečnosť, osobná bezpečnosť, spoločenská bezpečnosť a politická bezpečnosť (Kampová a Hollá, 2013).

Zdravie patrí medzi najcennejšie hodnoty človeka. Hrozby súvisiace s bezpečnosťou zdravia sa týkajú rozvojových aj priemyselne rozvinutých krajín. Vychádzajúc zo správy Organizácie spojených národov spôsobujú nákazlivé a parazitické choroby v rozvojových krajinách 17 miliónov úmrtí ročne (UNDP, 1994).

Kľúčovými opatreniami predchádzania infekčným ochoreniam sú hygiena, sanitácia, výživa, zabezpečenie pitnej vody, budovanie kanalizácie, zlepšenie dopravnej infraštruktúry, technológií tranzitu a skladovanie potravín a odstránenie podvýživy. Nedostatočná realizácia uvedených opatrení predstavuje kritický faktor v dosahovaní vyššej úrovne bezpečnosti zdravia. V rozvinutých krajinách predstavujú najvážnejšie ochorenia ohrozujúce život človeka, kardiovaskulárne choroby, ktoré sú spájané s rýchlym životným štýlom a neprimeranými stravovacími návykmi, ako aj rakovinové ochorenia, ktoré bývajú často dôsledkom environmentálnych rizík (Kampová a Hollá, 2013).

Za to, že sa dĺžka života človeka tak výrazne zvýšila, môže predovšetkým zdravotná starostlivosť a pokrok medicíny. Pokrok medicíny a jej úroveň je možné považovať za atribút súčasnej civilizácie. Avšak to, ako je medicína využívaná v prospech človeka, nie je otázkou medicíny, ale priorít danej spoločnosti a organizácie zdravotnej starostlivosti (Porada a kol.,

2019). Pre zaistenie bezpečnosti zdravia je nevyhnutná dostupná zdravotná starostlivosť. Ide o kľúčový indikátor bezpečnosti zdravia (Kampová a Hollá, 2013). Tieto indikátory je možné klasifikovať nasledovne: (Tabuľka 1).

Tabuľka 1 Indikátory bezpečnosti zdravia

Kategória	**Indikátory**
Zdravotný stav	subjektívny pocit zdravia, zdravotné podmienky, stav invalidity, pravdepodobnosť mortality
Nemedicínske činitele zdravia	správanie sa človeka (fajčenie, alkohol, stravovanie, ...), životné a pracovné podmienky, osobné charakteristiky, environmentálne faktory
Výkonnosť zdravotného systému	dostupnosť, prijateľnosť, kompetentnosť, primeranosť, kontinuita, efektivita, bezpečnosť
Spoločnosť a charakteristiky zdravotného systému	spoločnosť (počet a hustota obyvateľov, menšiny, počet obyvateľov žijúcich v mestách, ...), zdravotný systém, zdroje (počet doktorov, špecialistov, zdravotných sestier)

Zdroj: Canadian Institute for Health Information, 2012

Špecifickým indikátorom bezpečnosti zdravia je charakteristika konkrétneho ochorenia, ktorá sa popisuje prostredníctvom incidencie, prevalencie, ako aj priemernej doby daného ochorenia (Le, a kol., 1994). *„Incidencia určuje počet novovzniknutých prípadov ochorenia, ktoré sa prejavili v priebehu určitého času k celkovej veľkosti populácie. Incidencia tak definuje riziko vzniku ochorenia počas definovaného obdobia. Prevalencia udáva počet chorých k určitému okamihu a vypočítava sa ako pomer všetkých osôb s ochorením k dátumu zisťovania voči populácii. Vzťah medzi incidenciou a prevalenciou sa definuje ako priemerná doba ochorenia"* (Kampová a Hollá, 2013, s. 22).

2 RIZIKO ZDRAVOTNÝCH HROZIEB V PONÍMANÍ BEZPEČNOSTNEJ STRATÉGIE SLOVENSKEJ REPUBLIKY

Bezpečnostná stratégia Slovenskej republiky definuje ako životne dôležité bezpečnostné záujmy Slovenskej republiky zachovanie jej nezávislosti, zvrchovanosti, územnej celistvosti a nedotknuteľnosti hraníc, právneho štátu a demokratického ústavného zriadenia, ako aj **ochranu života a zdravia**, základných práv a slobôd jej obyvateľov. Globálne zdravotné hrozby môžu nadobudnúť podobu nepredvídaného a nekontrolovaného ohrozenia verejného zdravia. Krízové a mimoriadne situácie môžu byť vyvolané biologickými, chemickými alebo fyzikálnymi faktormi, či prírodnými, humanitárnymi krízami a katastrofami, ako aj rozličnými konfliktami destabilizujúcimi politické, hospodárske a sociálne systémy a ohrozujúce zdravotnú starostlivosť pre obyvateľstvo, vrátane jeho imunizácie. Riziko globálneho šírenia nákazy zvyšuje vysoká mobilita ľudí a nepripravenosť systému verejného zdravotníctva reagovať na ohrozenia a mimoriadne udalosti.

Z tohto dôvodu je potrebné koordinovane monitorovať zdroje nákazy a reagovať na jej šírenie. Vzhľadom na uvedené Bezpečnostná stratégia Slovenskej republiky nastavuje ciele v oblasti ochrany verejného zdravia v rozsahu adekvátnej zdravotnej starostlivosti. Táto sa týka nie len ochrany zdravia občanov Slovenskej republiky pred pandémiami, radiačnými a ekologickými haváriami, ale aj akcieschopnosti pri výskyte prírodných katastrof, teroristických útokov či iných ohrozeniach bezpečnosti štátu. Základom na zabezpečenie

vysokej úrovne ochrany verejného zdravia sú monitorovanie, včasné varovanie a nadväzujúce opatrenia pri mimoriadnych ohrozeniach zdravia. Prioritou musí byť zefektívnenie súčasných národných a európskych systémov na zabezpečenie ochrany verejného zdravia.

V rámci Svetovej zdravotníckej organizácie je potrebné aby Slovenská republika prispievala k posilneniu medzinárodnej koordinácie a spolupráce pri zvyšovaní pripravenosti a odolnosti štátov voči budúcim krízam ohrozujúcim zdravie populácie, ako riešenia dlhodobých štrukturálnych výziev zdravotných systémov na princípe solidarity. Pripravenosť zdravotníctva v Slovenskej republike závisí od zachovania a posilnenia kritickej infraštruktúry v kontexte zabezpečenia personálnych síl a prostriedkov pri ochrane verejného zdravia a poskytovaní zdravotnej starostlivosti. Cieľom je udržanie adekvátneho lôžkového fondu a primeranej kapacity záchrannej zdravotnej služby, špecializovaných medicínskych pracovísk a laboratórií, či dostatočnú úroveň personálneho a materiálneho vybavenia úradov verejného zdravotníctva, zásob a zásobovania zdravotníckym materiálom a liekmi (Bezpečnostná stratégia Slovenskej republiky, 2021).

3 OHROZENIE ZDRAVIA Z POHĽADU EURÓPSKEJ ÚNIE

Výskyt infekčných ochorení sa oproti dávnej minulosti znížil, napriek tomu sa aj v súčasnosti vyskytujú ohrozenia, či už v podobe pandémie chrípky (H1N1) v roku 2009, epidémie baktérie E. coli v roku 2011, vírusu Ebola v západnej Afrike v roku 2004, vírusu Zika v roku 2016 a aktuálneho ochorenia COVID-19. Tieto ochorenia dokazujú, že aj v súčasnosti môžu nové infekcie spôsobiť medzinárodné ohrozenie zdravia. Zamedzenie šírenia cezhraničných ohrození zdravia vyžaduje pripravenosť štátov a koordinované opatrenia. Reakcia na ohrozenie zdravia by mala zahŕňať jednak odhaľovanie a identifikáciu ohrozenia a následne zriadenie kanálov včasného varovania prostredníctvom postupov, ktoré môžu zdravotnícke orgány použiť na cielenú výmenu informácií.

Posudzovanie rizík je podstatným prvkom pri rozhodovaní, či a ako reagovať na hrozbu. Dlhodobé hrozby vyžadujú zavedenie cielených opatrení. Takouto hrozbou sa môže javiť aj antimikrobiálna rezistencia, ktorá vyžaduje primeranú úroveň pripravenosti a reakcie, alebo epidémie chorôb, ako sú HIV/AIDS, vírusová hepatitída a tuberkulóza.[1]

3.1 EURÓPSKY ÚRAD PRE PRIPRAVENOSŤ A REAKCIE NA NÚDZOVÉ ZDRAVOTNÉ SITUÁCIE (HERA)

Za účelom posilnenia pripravenosti Európskej únie na riešenie situácií týkajúcich sa ohrozenia zdravia a koordinácie zdravotnej bezpečnosti navrhla Európska komisia nový rámec pre bezpečnosť verejného zdravia, kedy bol zriadený **Európsky úrad pre pripravenosť a reakcie na núdzové zdravotné situácie (HERA)**. Úrad HERA začal fungovať ako nové generálne riaditeľstvo Európskej komisie dňa 16. septembra 2021. Jeho úlohou je posilniť schopnosť Európy predchádzať cezhraničným ochoreniam zdravia, prípadne ich včas odhaľovať a primerane na ne reagovať. Vo fáze pripravenosti je úlohou HERA usmerňovať opatrenia na zvýšenie prevencie, zlepšenie pripravenosti a reakcieschopnosti a v krízovej fáze môže využívať právomoci na rýchle rozhodovanie a vykonávanie núdzových opatrení.[2]

[1] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en
[2] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en

3.2 ROZHODNUTIE O ZÁVAŽNÝCH CEZHRANIČNÝCH OHROZENIACH ZDRAVIA

Európska únia taktiež priebežne zavádza právne predpisy za účelom zjednotenia postupov pri cezhraničnom ohrození zdravia spôsobeným infekčnými chorobami. Kľúčovým bolo v tejto súvislosti prijatie **rozhodnutia 1082/2013/EÚ Európskeho parlamentu a Rady z 22. októbra 2013 o závažných cezhraničných ohrozeniach zdravia**, ktorého cieľom bolo zlepšiť pripravenosť a posilniť kapacity na koordinovanú reakciu na núdzové situácie v oblasti zdravia v rámci Európskej únie. Ide o dôležitý právny predpis, ktorý zlepšil zdravotnú bezpečnosť v Európskej únii. Podporil členské štáty Európskej únie v boji proti cezhraničným hrozbám a ochranu občanov pred možnými pandémiami prostredníctvom posilnenia kapacity na plánovanie pripravenosti na úrovni Európskej únie, prevádzkovania systému včasného varovania na hlásenie závažných cezhraničných ohrození zdravia, zlepšovania posudzovania rizika a riadenia cezhraničných ohrození zdravia, vykonávania spoločného obstarávania týkajúceho sa zdravotníckych protiopatrení, zlepšenia koordinácie celoeurópskej reakcie poskytnutím solídneho zákonného mandátu Výboru pre zdravotnú bezpečnosť a podpory medzinárodnej spolupráce a celosvetových opatrení.[3]

Prijatie Rozhodnutia 1082/2013/EÚ bolo dôležité taktiež z dôvodu sfunkčnenia siete pre epidemiologický dohľad nad prenosnými chorobami a súvisiacimi špeciálnymi zdravotnými problémami. Vychádzajúc z článku 8 rozhodnutia 1082/2013/EÚ je úlohou Európskej komisie zabezpečiť informovanosť, resp. rýchle varovanie na úrovni Európskej únie o závažných cezhraničných ochoreniach zdravia prostredníctvom **Systému včasného varovania a reakcie (EWRS)**. Tento je použiteľný na varovanie, zdieľanie informácií a koordináciu opatrení v reakcii na predchádzajúce prepuknutia SARS, pandemickej chrípky (H1N1), Ebola, Zika, COVID-19, či iných cezhraničných ohnísk prenosných chorôb.[4]

Na základe skúseností získaných pri riešení krízy koronavírusu bol predložený **Návrh nariadenia o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie 1082/2013/EÚ**, ktorý vytvára spoľahlivý mandát na koordináciu na úrovni Európskej únie.[5]

3.3 EURÓPSKE CENTRUM PRE PREVENCIU A KONTROLU CHORÔB A EURÓPSKA AGENTÚRA PRE LIEKY

Európske centrum pre prevenciu a kontrolu chorôb (ECDC) je agentúra Európskej únie zameraná na posilnenie obranyschopnosti Európy proti infekčným chorobám, ktorého úlohou je identifikovať, posudzovať a oznamovať vznikajúce, ale aj súčasné hrozby pre ľudské zdravie v podobe infekčných chorôb.

Úlohou ECDC je testovať a vykonávať audit plánov pripravenosti na pandémiu na úrovni Európskej únie, ako aj na vnútroštátnej úrovni. Pri svojom dohľade by malo využívať umelú inteligenciu a ďalšie technologické prostriedky. Mandát ECDC by mal byť posilnený o epidemiologický dohľad prostredníctvom integrovaných systémov, ktoré umožňujú dohľad v reálnom čase, poskytovanie nezáväzných odporúčaní a možností riadenia rizík, schopnosť nasadiť tímy pomoci Európskej únie pri vypuknutí pandémie, či budovanie siete referenčných laboratórií Európskej únie.[6]

Európska agentúra pre lieky (EMA) je agentúrou hodnotiacou a monitorujúcou lieky v rámci Európskej únie a Európskeho hospodárskeho priestoru. Jej cieľom je poskytovať

[3] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en
[4] https://health.ec.europa.eu/health-security-and-infectious-diseases/surveillance-and-early-warning_en
[5] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en
[6] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en

vedecké poradenstvo o liekoch, koordinovanie štúdií vo vzťahu k zisťovaniu účinnosti a bezpečnosti očkovacích látok, či koordinovanie klinického skúšania.[7]

ZÁVER

Problematika globálnych zdravotných hrozieb predstavuje v posledných rokoch jednu z často diskutovaných tém. Zdravotné hrozby môžeme považovať za plnohodnotnú bezpečnostnú hrozbu, ktorá bude vo svete prítomná aj nastávajúce obdobie.

Šírenie infekčných ochorení a samotné zdravotné hrozby úplne nezastavíme, preto musíme vedieť na takéto hrozby adekvátne reagovať. Základom na zabezpečenie ochrany verejného zdravia sú monitorovanie, včasné varovanie a nadväzujúce cielené opatrenia pri mimoriadnych ohrozeniach zdravia. Prioritou musí byť taktiež zefektívnenie národných a európskych systémov na zabezpečenie ochrany verejného zdravia. Na národnej úrovni je potrebné neustále skvalitňovanie zdravotnej starostlivosti a jej dostupnosť. Na medzinárodnej úrovni je nutné reagovať vytváraním inštitúcií a dopĺňaním ich kompetencií tak, aby boli spôsobilé reagovať na nové hrozby, resp. monitorovať už existujúce a zabezpečovať včasnú informovanosť. Riešenie zdravotných hrozieb musí byť teda koordinovanou činnosťou na niekoľkých úrovniach a v neposlednom rade je dôležité zapojiť taktiež aj samotných obyvateľov.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

Knihy a monografické publikácie

HOFREITER, L. – BYRTUSOVÁ, A., 2016. *Indikátory bezpečnosti.* Zlín: Radim Bačuvčík – VeRBuM, 2016, 136 s. ISBN 978-80-87500-82-8.

KAMPOVÁ, K. – HOLLÁ, K., 2013. *Manažment sociálnych rizík*. Žilina: Žilinská univerzita v Žiline, 2013, 108 s. ISBN 978-80-554-0754-8.

LE, C. T. – BOEN, J. R., 1994. *Health and Numbers: Basic Biostatistical Methods*. Chichester: John Wiley & Sons, 1994, ISBN 978-0-471-01248-1.

PORADA, V. a kol., 2000. *Úvod do teórie činnosti policajno-bezpečnostných orgánov*. Bratislava: Akadémia Policajného zboru, 2000, ISBN 80-8054-153-1.

PORADA, V. a kol., 2019. *Bezpečnostní vědy: Úvod do teorie, metodologie a bezpečnostní terminologie*. Plzeň: Aleš Čeněk, s. r. o., 2019, 780 s. ISBN 978-80-7380-758-0.

VOLNER, Š., 2005. *Nová teória bezpečnosti: Teoreticko-metodologické východiská.* Zvolen: Bratia Sabovci, s. r. o., 2005, 340 s. ISBN 80-89029-99-X.

Stratégie a dokumenty

BEZPEČNOSTNÁ STRTÉGIA SLOVENSKEJ REPUBLIKY. 2021. [cit. 2022-09-10]. Dostupné na internete: <https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf >.

CANADIAN INSTITUTE FOR HEALTH INFORMATION, 2012. *Health Indicators 2012*. Ottawa: CIHI, 2012, ISBN 978-1-77109-047-6.

[7] https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en

Rozhodnutie Európskeho parlamentu a Rady 1082/2013/EÚ z 22. októbra 2013 o závažných cezhraničných ohrozeniach zdravia. [cit. 2022-09-10]. Dostupné na internete: < https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32013D1082>.

UNDP, 1994. *Human development report 1994*. New York: Oxford University Press, 1994, ISBN 0-19-509170-1.

Internetové stránky

EURÓPSKA KOMISIA. [cit. 2022-09-10]. Dostupné na internete: <https://health.ec.europa.eu/health-security-and-infectious-diseases/overview_en>.

EURÓPSKA KOMISIA. [cit. 2022-09-10]. Dostupné na internete: <https://health.ec.europa.eu/health-security-and-infectious-diseases/surveillance-and-early-warning_en>.

npor. JUDr. Michaela ŠIMONOVÁ
Externá doktorandka Katedry bezpečnosti a obrany
Akadémia ozbrojených síl generála M. R. Štefánika Liptovský Mikuláš
Demänová 393
031 01 Liptovský Mikuláš
E-mail: michaela.simonova1@gmail.com

DOPRAVNÉ SPÔSOBILOSTI OZBROJENÝCH SÍL SLOVENSKEJ REPUBLIKY V KONTEXTE POŽIADAVIEK NA STRATEGICKÚ PREPRAVU

TRANSPORT CAPABILITIES OF THE ARMED FORCES OF THE SLOVAK REPUBLIC IN THE CONTEXT OF STRATEGIC TRANSPORTATION REQUIREMENTS

Marián ŠIŠKA

ABSTRACT

The thesis deals with transportation capabilities of the Slovak Armed Forces in regard of strategic transportation requirements. The first chapter analyses strategic transportation. It specify what strategic transportation is, clarifies assured access to strategic transport capabilities, deals with processes of arranging strategic transport and identify demands imposed on the Armed Forces of the Slovak Republic. The second chapter is devoted to transportation capabilities. It analyses already achieved capabilities of all modes of transport in Slovak Ministry of Defence and talks about challenges Slovak defence sector is facing.

Keywords: strategic transportation, transport capabilities, transportation modes

ÚVOD

Slovenská republika je od roku 2004 členom Európskej únie a organizácie Severoatlantickej aliancie. Členstvo v uvedených zoskupeniach zo sebou prináša množstvo výhod a garancií ale aj záväzkov. Jedným zo záväzkov, ktorými je Slovenská republika viazaná, je aj jej angažovanosť v medzinárodných civilných a vojenských operáciách, ktoré prispievajú k zabezpečeniu medzinárodného mieru a stability vo svete.

Nasadzovanie jednotiek do medzinárodných operácií so sebou prináša aj potrebu zabezpečenia prepravy personálu, techniky a materiálu do stanovených priestorov pôsobenia. Aj keď EÚ a NATO presadzujú politiku spoločného prístupu k riešeniu konfliktov, zabezpečenie prepravných požiadaviek vlastných jednotiek je väčšinou v národnej zodpovednosti každej zúčastnenej krajiny.

Cieľom práce je analýza súčasne dosiahnutých dopravných spôsobilostí Ozbrojených síl Slovenskej republiky, ktorými zabezpečujú požiadavky na dopravné zabezpečenie vyplývajúce z pôsobenia v operáciách medzinárodného krízového manažmentu ako aj potenciálneho nasadenia deklarovaných príspevkov do síl rýchlej reakcie.

1 STRATEGICKÁ PREPRAVA

Rezort obrany Slovenskej republiky plní úlohy v súlade so zákonom č. 321/2002 Z.z. o Ozbrojených silách SR aj v operáciách mimo územia SR. Jednou z hlavných úloh je požiadavka na rozmiestnenie a následné komplexné logistické zabezpečenie predurčených jednotiek, ktorého súčasťou je aj zabezpečenie strategickej prepravy do a z miesta pôsobenia.

Strategickou leteckou prepravou rozumieme použitie vojenských strategických leteckých prostriedkov na prepravu materiálu, techniky a personálu na veľké vzdialenosti. V porovnaní s taktickou leteckou prepravou, ktorej úlohou je preprava v rámci určitého miesta pôsobenia, je strategická letecká preprava vykonávaná spravidla medzi kontinentmi a vyžaduje letecké prostriedky s väčšou prepravnou kapacitou.

Vznik požiadavky na zabezpečenie strategickej prepravy je zadefinovaný v kontexte medzinárodných záväzkov OS SR vyplývajúcich z národných cieľov 2017 ako cieľ spôsobilosti E 2201 Strategická preprava. OS SR sa akceptovaním uvedeného cieľa síl zaviazali zabezpečiť zaručenú dostupnosť (Short-Notice Assured Access) strategických prepravných kapacít pre prepravu národných deklarovaných jednotiek požadovaných NATO z určených letísk a prístavov nakladania v SR na letiská a do prístavov vykladania nachádzajúcich sa v operačnej oblasti.

Zabezpečenie zaručeného prístupu k strategickej preprave v krátkom čase pre požadované kapacity deklarovaných príspevkov je definované ako:

a) strategická letecká preprava:
   - zabezpečenie kapacity na prepravu 800 osôb s výzbrojou na vzdialenosť 2500 km do 10 dní;
   - zabezpečenie kapacity na prepravu 500 ton vojenskej techniky a materiálu na vzdialenosť 2500 km do 10 dní.

b) strategická námorná preprava:
   - zabezpečenie kapacity na prepravu techniky (1000 jednotiek LIM = merná jednotka pri preprave techniky) na vzdialenosť 6000 námorných míľ do 15 dní,
   - zabezpečenie kapacity na prepravu 250 ks kontajnerov (20´ ISO1C do 10 ton/kontajner) na vzdialenosť 6000 námorných míľ do 15 dní,
   - zabezpečenie kapacity na prepravu 1000 ks kontajnerov počas fázy udržiavania.

Strategická preprava pozostáva z troch častí:

1. národná časť presunu je realizácia prepravy osôb, techniky a materiálu z domácich základní do miesta nakladania (ďalej len „POE“, z angl. Port Of Embarkation), či už je to letisko alebo prístav. Je plne v národnej kompetencií každého členského štátu.
2. strategická časť presunu je preprava osôb, techniky a materiálu z POE do miesta vykladania (ďalej len „POD“, z angl. Port Of Debarkation). Strategickú časť presunu plánuje, koordinuje a dekonfliktuje najvyšší veliteľ spojeneckých síl v Európe (ďalej len „SACEUR“ = Supreme Allied Commander Europe), prostredníctvom Spojeneckého centra pre koordináciu presunov (ďalej len „AMCC“, z angl. Allied Movement Coordination Centre). Zabezpečenie prepravy vlastných jednotiek je v národnej zodpovednosti členských štátov.
3. operačná časť presunu je časť presunu z POD do konečného miesta pôsobenia jednotky. Zodpovednosť za operačnú časť presunu je rozdelená medzi:
   - veliteľa spoločných síl (JFC – joint force commander), ktorý plánuje a zabezpečuje prijatie, skladovanie a následný presun jednotiek (ďalej len „RSOM“, z angl. Recieving, Staging and Onward Movement), spolupracuje a koordinuje požiadavky na presun s hostiteľskou krajinou,
   - členský štát, ktorý plánuje na národnej úrovni, zodpovedá za zabezpečenie prepravy a vykonanie presunu v súlade s plánom veliteľa JFC.

2 DOPRAVNÉ SPÔSOBILOSTI OS SR

2.1 ŽELEZNIČNÁ PREPRAVA

Železničná doprava je schopná zabezpečiť prepravu nadrozmerného a ťažkotonážneho materiálu a techniky na veľké vzdialenosti pri relatívne vysokej rýchlosti. Jej prepravná kapacita závisí od viacerých faktorov, či už dostupnosť hnacích koľajových vozidiel (rušňov), železničných vozňov, ale aj nakladacia miera prepravovaného nákladu. Preprava rôznych typov techniky si vyžaduje obstaranie/objednanie rôznych druhov špeciálnych železničných vozňov, ktoré treba sústrediť a pristaviť na požadované miesto nakladania. Preto je potrebné železničnú prepravu plánovať v dostatočnom časovom predstihu. Neplánované prepravy po železnici nie sú možné.

Počas zabezpečenia medzinárodných železničných presunov dochádza k prechodu vlakových súprav do iných národných a regionálnych železničných sieti, ktoré môžu byť prevádzkované na základe vlastných národných predpisov a štandardov. Rozdiely v štandardoch sa spravidla týkajú rozchodu koľají, výšky mostov a nástupíšť, prejazdnosti tunelov alebo rýchlostných limitov. Z toho dôvodu je pri plánovaní železničnej prepravy potrebné dodržiavať najprísnejšie predpisy a normy štátu, cez ktorý bude vlak prechádzať.

Železničná preprava má vždy vopred stanovenú trasu. Je vymedzená existujúcimi železničnými traťami, čo môže byť veľmi limitujúce pri potrebe zabezpečiť prepravu materiálu a techniky do odľahlých alebo ťažšie dostupných priestorov nasadenia. Vybudovanie a položenie nových koľají je z časového ako aj finančného hľadiska neefektívne. Železničná preprava v podmienkach OS SR je preto vo väčšine prípadov plánovaná ako súčasť kombinovanej prepravy.

Rezort obrany SR v súčasnosti nedisponuje vlastnými hnacími koľajovými vozidlami ani železničnými vozňami. Ich dostupnosť je kontraktovaná prostredníctvom rámcovej dohody s civilným sektorom č. 2021/518 – cestná a železničná preprava, v rámci ktorej má Ministerstvo obrany SR uzatvorený kontrakt na poskytnutie prepravných služieb zabezpečujúcich medzinárodnú cestnú a železničnú prepravu nákladu a osôb. Rámcová dohoda je uzavretá s jedným poskytovateľom na dobu 48 mesiacov..

Ďalšou možnosťou zabezpečenia prepravných požiadaviek po železnici je využitie oddelenia pozemnej prepravy (ďalej len „IST“) v rámci projektu MCCE (ang. skratka: Movement Coordination Centre Europe). Projekt MCCE vznikol v roku 2007 ako reakcia na potrebu efektívnejšieho využívania prepravných prostriedkov členských krajín pri prepravách do a z operácií medzinárodného krízového manažmentu. Projekt MCCE plní funkciu stáleho medzinárodného koordinačného centra v oblasti prepravných kapacít členských štátov projektu; sústreďuje a používa aktuálne informácie o prepravných kapacitách a aktivitách členských štátov za účelom navrhnutia vhodnejšieho a efektívnejšieho zabezpečenia prepravných požiadaviek.

Princíp fungovania projektu je založený na zdieľaní prepravných kapacít medzi členskými štátmi s cieľom maximalizovať vyťaženie dopravného prostriedku, čo v konečnom dôsledku vedie k profitu všetkých zúčastnených strán podieľajúcich sa na preprave a k úspore finančných prostriedkov. Členské krajiny na báze dobrovoľnosti takisto zdieľajú v rámci projektu svoje dostupné dopravné možnosti. To znamená, že ktorýkoľvek členský štát projektu môže poskytnúť svoje prostriedky, či už vlastné alebo prenajaté, v prospech iného členského štátu za finančnú alebo nepeňažnú refundáciu.

2.2 NÁMORNÁ PREPRAVA

Námorná preprava spolu s leteckou prepravou patria z pohľadu strategickej prepravy za kľúčové pri nasadzovaní jednotiek do priestorov pôsobenia. Námorná preprava je charakteristická svojou veľkou prepravnou kapacitou, výkonom s ohľadom na objem prepravovaného materiálu, hospodárnosťou a rýchlosťou čo sa týka objemu prepraveného materiálu za určitý čas. Považuje sa za hlavný druh dopravy pri nasadení hlavných síl do priestorov operácie na iných kontinentoch. Jej hlavnými obmedzujúcimi faktormi sú pomalosť plavby a zraniteľnosť počas prepravy a v prístavoch.

Pri prvotnom nasadení síl do operácie sa prednostne využívajú veľkokapacitné lode typu RO-RO (z ang. skratky Rolled-on/Rolled-off), ktoré umožňujú horizontálne aj vertikálne nakladanie. RO-RO lode dokážu rýchlo naloditˊ rôzne typy vojenskej techniky a materiálu, a je možné ich v prípade potreby použiť na taktické nakladanie a vykladanie.

Pre zásobovanie operácií materiálom sú najčastejšie využívané lode typu LO-LO (z ang. skratky Loaded-on/Loaded-off), ktoré využívajú vertikálny (žeriavový) typ nakladania a sú primárne určené na prepravu materiálu v kontajneroch. Ich ponuka na trhu je značne vyššia ako pri RO-RO lodiach.

Ozbrojené sily SR nedisponujú vlastnými námornými dopravnými prostriedkami. Nakoľko je SR vnútrozemská krajina bez morskej hranice, ich prevádzka a využívanie pod velením Ozbrojených síl SR na území iného štátu by bolo značne komplikované. Rezort obrany nemá momentálne k dispozícii zaručený prístup k námorným prepravným kapacitám. V súčasnosti prebieha verejné obstarávanie pre zabezpečenie predmetu zákazky „Medzinárodná preprava“, v rámci ktorého bude obstarávaný aj prístup k námorným prepravným kapacitám v rámci kombinovanej prepravy.

Ďalším spôsobom zabezpečenia námornej prepravy pre potreby OS SR je členstvo v medzinárodnom projekte AMSCC (Athens Multinational Sealift Coordination Centre). AMSCC je medzinárodný projekt po vedením Grécka, ktorý zabezpečuje prístup k strategickej námornej preprave jeho členským krajinám. Bol založený v roku 2004 Gréckym ministerstvom obrany ako reakcia na rastúce potreby adekvátneho zabezpečenia námorných prepráv s ohľadom na efektívnosť vynaložených nákladov. AMSCC je nezisková organizácia zameraná na bezplatné poskytovanie informácií o ponukách jej obchodných dodávateľov.

AMSCC zabezpečuje strategické námorné kapacity na základe vyžiadania. Po predložení požiadavky AMSCC osloví v rámci vlastného obstarávacieho mechanizmu trh s námornými kapacitami a do troch dní predloží ponuku na zabezpečenie tejto prepravy – pričom daná krajina ju môže resp. nemusí prijať. Projekt AMSCC má v súčasnosti 10 členských krajín Európskej únie, ktoré s ním podpísali bilaterálne dohody (ďalej len „MoU“, z angl. Memorandum of Understanding). Zároveň má podpísané MoU s NATO/SHAPE a administratívnu dohodu s EÚ finančným mechanizmom ATHENA. V rámci členstva v projekte OS SR zatiaľ nevyužili služby, ale táto možnosť je deklarovaná v rámci cieľov spôsobilostí.

OS SR môžu pre zabezpečenie námornej prepravy využiť aj projekt MCCE, konkrétne jeho oddelenie námornej prepravy. Vďaka členstvu v projekte MCCE majú OS SR po dohode prístup k námorným prepravným prostriedkom ostatných členských krajín.

2.3 CESTNÁ PREPRAVA

Hlavnou charakteristickou vlastnosťou cestnej prepravy je jej flexibilita. Vo všeobecnosti sa dá povedať, že je len málo miest, do ktorých sa nedá dostať po ceste. Pre zabezpečenie strategickej prepravy sama o sebe však nie je vhodná. Jej využitie sa nájde skôr pri prepojení ostatných druhov prepráv, a to hlavne v začiatočnej fáze (presun z domovských kasárni do POE) a v konečnej fáze, pri presune z POD do operačného priestoru. Cestnú dopravu

limituje najmä relatívne nízka prepravná kapacita na veľké vzdialenosti s ohľadom na potrebné ľudské zdroje pre jej zabezpečenie.

Cestná preprava v podmienkach OS SR je zabezpečovaná prevažne vlastnými silami a prostriedkami. Ďalšími možnosťami zabezpečenia dopravných požiadaviek na cestnú prepravu sú využitie služieb zmluvného prepravcu Ministerstva obrany SR, na základe rámcovej dohody č. 2021/518 alebo prostredníctvom projektu MCCE v rámci oddelenia IST.

Cestná preprava je najčastejšie využívaným druhom dopravy na taktickom stupni. Základnou požiadavkou na rozvoj dopravných spôsobilostí cestnej prepravy, je vytvorenie jednotiek, ktoré budú schopné efektívne plniť dopravné úlohy v pridelenom priestore operácie. V tabuľke nižšie sú uvedené súčasné dosiahnuté spôsobilosti cestnej dopravy v rezorte obrany SR, vyplývajúce z koncepcie rozvoja dopravných spôsobilosti v súlade so Základným modelom OS SR 2030 a so štandardmi interoperability NATO v oblasti dopravného zabezpečenia.

Tabuľka 1: Súčasné spôsobilosti cestnej prepravy v rezorte obrany SR

Spôsobilosť	**Hlavné operačné požiadavky**	**Súčasný stav**
Jednotka železničných operácií (RSOM-ROU)	- schopnosť manipulácie patetizovaného aj nepatetizovaného materiálu a prepravných kontajnerov v železničných termináloch, - zmanipulovanie 500 ks techniky alebo 2.500t nákladu alebo ich kombinácia, - schopnosť spolupráce s vojenskými a civilnými organizáciami.	jednotka nie je v dlhodobých plánoch štruktúr OS SR z dôvodu nevyužiteľnosti pre účely OS SR. Nutná investícia do výcviku personálu a nákup špeciálnej techniky.
Stredná dopravná rota (velenie + 3x dopravná čata; celkom 60 PrV)	- schopnosť zabezpečiť cestnú prepravu po stanovených trasách, po spevnených aj nespevnených komunikáciách, - schopnosť prepraviť 600 ton kontajnerovaného nákladu alebo iné druhy nákladu na vzdialenosť 300 km denne.	Dopravná rota je deklarovaná v počte 42 PrV (koeficient 0,6) v štruktúre 53. práporu poľných služieb Hlohovec v zložení: velenie roty 2x dopravná čata
Dopravná rota PHM	- schopnosť zabezpečiť cestnú prepravu nebalenej PHM (500m^3) na vzdialenosť 300 km denne po spevnených aj nespevnených komunikáciách, - schopnosť prijímať a vydávať PHM cez spojky alebo autorizované adaptéry podľa potreby.	1x dopravná rota zložená z 2 čiat prepravy PHM a velenia, celkom 40 PrV, v štruktúre 53. práporu poľných služieb Hlohovec.
2x tím riadenia presunov (RSOM)	- schopnosť riadiť presuny v rámci cestnej siete v pridelenom priestore operácie	Tím riadenia presunov je vytvorený 1x (sily vyššej pripravenosti s dobou pohotovosti 60 dní) a 1x (sily nižšej pripravenosti s dobou pohotovosti 180 dní) v štruktúre 53. práporu poľných služieb Hlohovec
Dopravná rota v zložení: 2x dopravná čata 1x dopravná čata PHM 1x čata prepravy vody	- spôsobilosť uložiť 450t materiálu ZT I, II a IV; 300m^3 ZT III a 3xDOS ZT V. - spôsobilosť prepraviť 125t nákladu, 110m3 PHM a 400m3 vody a 2xDOS ZT V na vzdialenosť 90km denne.	Dopravná rota je vytvorená v štruktúre 53. práporu poľných služieb Hlohovec. Súčasný stav techniky nezodpovedá kladeným požiadavkám. Nevyhnutné doplnenie techniky na tabuľkové počty a obnova zastaranej techniky.
3x čata ťažkej prepravy v zložení: 3x družstvo ťažkej prepravy	- spôsobilosť prepravy ťažkej obrnenej techniky, napr. BVP a bojové tanky.	1x čata vytvorená v štruktúre 53. práporu poľných služieb Hlohovec v zložení: 2x družstvo ťažkej prepravy

Zdroj: vlastné spracovanie

2.4 LETECKÁ PREPRAVA

Letecká preprava je takmer vždy nevyhnutná pre zabezpečenie vojenských operácií. Jej flexibilita, schopnosť prekonávať veľké vzdialenosti, rýchlosť a variabilnosť z nej robia ideálny druh prepravy, umožňujúci rýchle nasadenie jednotiek do priestoru pôsobenia.

Ozbrojené sily SR v súčasnosti nedisponujú strategickými leteckými prostriedkami. Aktuálne majú OS SR dostupné taktické letecké prostriedky stredného doletu, ktoré sú schopné zabezpečiť jednotlivé prepravné požiadavky ktoré sú primárne dislokované v dopravnom krídle Kuchyňa:

- C-27 J Spartan v počte 2,
- L-410 Turbolet v počte 7,

Nakoľko Slovenská republika nemá strategické letecké prostriedky, zaručená dostupnosť strategických leteckých kapacít vyplývajúca z medzinárodných záväzkov a národných cieľov 2017 je v súčasnosti čiastočne zabezpečovaná využívaním prostriedkov Leteckého útvaru Ministerstva vnútra SR (ďalej len „LÚ MV SR“), členstvom SR v projekte SALIS, zmluvným prepravcom MO SR a čiastočne aj prostredníctvom projektu MCCE.

Členstvom v projekte MCCE si OS SR rozšírili možnosti zabezpečenia svojich prepravných požiadaviek prostredníctvom všetkých druhov dopravy, vrátane leteckej. Úlohou projektu MCCE je vyhľadávať možnosti zdieľania prepravných kapacít, ich vzájomné spájanie a koordinovanie jednotlivých prepráv. Členské krajiny sa prostredníctvom denne aktualizovaného informačného systému vzájomne informujú o dostupných prepravných kapacitách. MO SR takto získava aktuálny prehľad o efektívnych a finančne výhodných riešeniach pre zabezpečenie svojich prepravných požiadaviek.

Projekt SALIS (Strategic Air Lift International Solutions) je mnohonárodné konzorcium 9 krajín, ktoré vzniklo za účelom zabezpečenia zaručeného prístupu členských krajín k strategickým leteckým prostriedkom Antonov AN-124-100 pre ich využitie v prospech operácií medzinárodného krízového manažmentu pod záštitou NATO a Európskej únie.

Projekt SALIS poskytuje zaručený prístup k strategickej leteckej prepravnej kapacite, ktorá je garantovaná zaručenou dostupnosťou dvoch leteckých prostriedkov AN-124-100 pre ktorúkoľvek členskú krajinu do 72 hodín od ich vyžiadania. Ďalšie tri letecké prostriedky majú zaručenú dostupnosť do šesť, respektíve deväť dní od zadania požiadavky na prepravu. Tieto letecké prostriedky majú svoju domovskú základňu na letisku v Lipsku (Nemecko) a sú využiteľné v prípade potreby rýchleho nasadenia jednotiek alebo techniky do operácií NATO a EÚ.

Prednosťou projektu SALIS sú najmä prepravné schopnosti leteckého prostriedku AN-124-100, ktoré dokáže prepraviť až do 100 ton nákladu na veľkú vzdialenosť. Takisto jeho nákladový priestor je prispôsobený na prepravu nadrozmerného nákladu, vďaka čomu je vhodné na prepravu bojovej techniky ako napríklad tanky, bojové vozidlá pechoty ale aj vrtuľníky.

Nevýhodou projektu je, že v prípade potreby veľkého počtu letov viacerých členských krajín za rovnaké časové obdobie, nemusí 5 kontraktovaných leteckých prostriedkov postačovať na pokrytie prepravných požiadaviek všetkých krajín zapojených do projektu a to z časového alebo kapacitného hľadiska.

Letecký útvar Ministerstva vnútra SR je vládna letecká spoločnosť Slovenskej republiky so sídlom v Bratislave. Ministerstvo obrany SR ma uzatvorenú Zmluvu o vzájomnej spolupráci s Ministerstvom vnútra SR. Na základe tejto zmluvy má MO SR prístup k leteckým prostriedkom Leteckého útvaru Ministerstva vnútra SR Airbus A-319CJ a Fokker 100.

Letecké prostriedky Leteckého útvaru MV SR sú v súčasnosti využívané Ministerstvom obrany SR na strategickú leteckú prepravu personálu pôsobiaceho v operáciách NATO a OSN.

Nakoľko sú predmetné letecké prostriedky primárne určené na prepravu vládnych a ústavných činiteľov, prepravným požiadavkám MO SR nie je garantovaný zaručený prístup.

Ďalším spôsobom ako OS SR zabezpečujú svoje prepravné požiadavky v oblasti strategickej leteckej prepravy, je využívanie služieb zmluvného prepravcu MO SR. Služby zmluvného prepravcu MO SR sú ale limitované dohodnutou finančnou sumou, ktorú nesmie MO SR prekročiť počas doby platnosti kontraktu. Ďalším obmedzujúcim faktorom pre OS SR pri zabezpečovaní požiadaviek na strategickú leteckú prepravu je, že zmluvný prepravca MO SR negarantuje zaručený prístup k svojim vlastným prepravným prostriedkom ani k prepravným prostriedkom svojich subdodávateľov. MO SR v súčasnosti nemá uzatvorený kontrakt so žiadnym zmluvným prepravcom. Aktuálne prebieha príprava súťažných podkladov pre otvorenie verejnej súťaže na predmet zákazky „Medzinárodná preprava“, v rámci ktorej bude súťažená aj letecká preprava osôb a nákladu, s predpokladom uzatvorenia novej rámcovej dohody v priebehu roka 2023.

ZÁVER

Dosiahnutie požadovaných úrovní dopravných spôsobilosti v Ozbrojených silách SR je dôležitým záujmom rezortu obrany nielen z pohľadu zabezpečenia úloh plnených v rámci domáceho krízového manažmentu, ale aj z pohľadu záväzkov, ktoré má Slovenská republika voči medzinárodným zoskupeniam, ktorých je členom. Vyhovujúce dopravné spôsobilosti sú nevyhnutné pre zabezpečenie činnosti Ozbrojených síl SR či už pri plnení úloh na území štátu alebo v medzinárodnom prostredí.

Neustále sa vyvíjajúce globálne bezpečnostné prostredie prináša so sebou aj nové konflikty a bezpečnostné hrozby pre krajiny EÚ a NATO. Reakcia na ne si vyžaduje komplexný prístup všetkých členských krajín, vrátane Slovenskej republiky. Jednou z hlavných úloh pre nasadenie jednotiek OS SR v rámci reakcie na krízovú situáciu, je aj zabezpečenie prepravy pre určené jednotky a zabezpečenie ich mobility v priestore pôsobenia. Pre splnenie tejto úlohy je nevyhnutné mať vybudované komplexné dopravné spôsobilosti všetkých druhov.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ATARES. 2015. *Technical Arrangement regarding Mutual Support through Exchange of Services in the realm of air force activity.*

EUROPEAN COMMISSION. *Joint communication to the European Parliament and Council – Improving Military Mobility in the European Union*. 2017.

GENERÁLNY ŠTÁB OS SR. 2015. *Metodické pokyny NGŠ OS SR pre systém zabezpečovania a čerpania letových hodín v súlade s členstvom SR v podprojekte ATARES projektu MCCE*.

GENERÁLNY ŠTÁB OS SR. 2015. *Spoločná vojenská doktrína – Dopravná logistika Ozbrojených síl SR VDJ-40-40(B)*.

GENERÁLNY ŠTÁB OS SR. 2018. *Koncepcia rozvoja dopravných spôsobilostí.* Č.: NCVD-54-8/2018.

GENERÁLNY ŠTÁB OS SR. 2018. *Plán NGŠ OS SR na prípravu, nasadenie, udržanie, stiahnutie a obnovu bojaschopnosti deklarovaných síl OS SR pre V4 EU BG*, č.: ŠbSP-26-3/2018

GENERÁLNY ŠTÁB OS SR. 2022. *Informačná správa pre náčelníka generálneho štábu OS SR – Medzinárodný projekt SALIS – uzatvorenie dodatku k zmluve medzi NSPA a ALS,* č.: 701.CVD-76-11/2022-OMPP

INFROMAČNÁ SPRÁVA. 2016. *Informácia NGŠ OS SR pre ministra obrany SR k projektu SALIS.* č. p.: NCVD-61-43/2016.

MINISTERSTVO OBRANY SR. 2021. *Rámcová dohoda č. 2021/518*. Č. p.: ÚpIA-EL3/1-66-31/2021-OOPS

SLOVENSKÝ OBRANNÝ ŠTANDARD. 2011. *2468 AMovP-4: Technické hľadiská prepravy vojenských zásielok po železnici.*

kpt. Mgr. Marián ŠIŠKA
externý doktorand Katedry bezpečnosti a obrany
AOS gen. M. R. Štefánika
Demänovská 393, 031 01 Liptovský Mikuláš
Marian.Siska@mil.sk, Marian.Siska24@gmail.com

O HYBRIDNÝCH HROZBÁCH A HYBRIDNEJ VOJNE

ON HYBRID THREATS AND HYBRID WAR

Róbert TOMÁŠEK

ABSTRACT

Organizations, institutions, as well as the population of the states of EU are increasingly subjected to cyber-attacks, which aim to dismantle and destroy democratically functioning societies and institutions from the inside and achieve the attacking actors´own goals through chaos and anarchy. The virtual environment represents a very specific and from the point of view of security, challenging environment in which todays´ war takes place.

Keywords: security, threats, risks, hybrid threats, hybrid war

ÚVOD

Dynamický a turbulentný vývoj súčasnej ľudskej spoločnosti so sebou prináša mnohé pozitívne, ale zároveň aj negatívne skutočnosti, ktoré sa prejavujú v rôznych oblastiach života človeka i celej ľudskej civilizácie. Dôkazom toho sú početné pôvodné i novo sa objavujúce bezpečnostné hrozby a riziká, ktoré oprávnene stavajú otázky bezpečnosti na popredné miesto (Ivančík, 2021a, s. 32). Bezpečnosť totiž tvorí základnú a nevyhnutnú podmienku rozvoja každej spoločnosti a dnes, v ére prehlbujúcej sa globalizácie, už neexistuje oblasť spoločenského života, ktorá by s ňou nebola spojená. Aj preto aktuálne patrí bezpečnosť k najviac frekventovaným a skloňovaným pojmom vo všetkých jeho podobách (Ivančík, 2022, s. 7).

Zvlášť v súčasnej Európe, kde sa síce nebojuje priamo na území konkrétneho štátu (okrem Ukrajiny!), ale bojuje sa v ešte náročnejšom a komplikovanejšom „prostredí“ – vo virtuálnom svete. Kybernetické útoky predstavujú veľmi efektívny účinný druh hrozieb patriaci medzi tzv. hybridné hrozby, ktoré narúšajú bezpečnosť členských štátov Európskej únie (ďalej len „EÚ“). Primárnym problémom pre európske štáty začala byť ochrana a zaisťovanie bezpečnosti proti hybridným hrozbám (nielen zo strany Ruska), čo významným spôsobom ovplyvnilo aj ich vzájomné vzťahy a spoluprácu.

Už niekoľko rokov predstavujú kybernetické útoky, resp. útočné kybernetické operácie [1] vedené na rôzne inštitúcie, organizácie, kritickú infraštruktúru, ako aj celú spoločnosť, jej ovplyvňovanie cez pretváranie a deformovanie verejnej mienky, ako aj vnútorných záležitostí jednotlivých štátov, za veľmi závažnú bezpečnostnú hrozbu, ktorá vďaka neustálemu zdokonaľovaniu informačných a komunikačných technológií [2], novým

[1] Útočné kybernetické operácie predstavujú kybernetické operácie vedené vojenskými alebo polovojenskými silami, pod velením a/alebo pod kontrolou štátov alebo neštátnych aktérov, zamerané na využitie slabých stránok protivníka, jeho zraniteľností, implementáciu rôznych techník narúšania kyberpriestoru, schopnosť preťažiť ťažko dostupné kybernetické ciele a presadzovanie cielených škodlivých kybernetických produktov (Ivančík, 2021b, s. 3)

[2] Sektor informačných a komunikačných technológií v súčasnosti predstavuje jednu z najrýchlejšie sa rozvíjajúcich oblastí spoločnosti. Výrazne sa premieta nielen do súkromnej a hospodárskej sféry, ale čoraz viac

spôsobom „virtuálneho konzumného“ spôsobu fungovania spoločnosti a fenoménom ako je globalizácia, zbrane hromadného ničenia, atď. naberá na intenzite a závažnosti. Aktéri týchto útokov sú ťažko identifikovateľní, pričom ide o štátnych aj neštátnych aktérov, ktorí majú rôzne motívy a ciele.

Ako uvádza Jurčák a kol. (2017), v súčasnosti po odstránení bipolarity sveta, je bezpečnostné prostredie stále komplikovanejšie a charakterizuje ho nestabilita a nerovnomernosť vývoja i vysoká dynamika. Možnosti ako destabilizovať štát, zasiahnuť obyvateľstvo alebo zničiť kritickú infraštruktúru už nie je otázkou použitia strategických jadrových nosičov a rozsiahlych operácií, ale zahrňujú laptopy, počítačové siete, pašované chemické, biologické, rádioaktívne látky, ktoré môžu byť na cieľ dopravené akýmkoľvek spôsobom, cielenú propagandu, organizovaný zločin. V súčasnosti sa už v diplomatických, politických, vojenských i akademických kruhoch nehovorí len o otvorených hrozbách, ale čoraz častejšie aj o hrozbách asymetrických, zámerných, latentných, permanentných – hybridných hrozbách.

1 HROZBA A RIZIKO

Riziká a hrozby sú spojené so životom človeka od počiatku. Vždy tu existovali tzv. primárne riziká ako napr. prírodné živly, choroby, divá zver. Postupne ako sa vyvíjal človek a spoločnosť, spolu s nimi sa začali vyvíjať aj tzv. sekundárne riziká, ktorých pôvodcom bol sám človek.

Pojmy riziko a hrozba sa často pri rôznych príležitostiach zamieňajú, pričom dochádza k nesprávnej interpretácii v kontexte bezpečnostných rizík a bezpečnostných hrozieb. Ako uvádza Laml (2008), vo vzťahu rizika a hrozby existujú tri prístupy na vymedzenie ich vzťahov:

- synomymické (pojmy majú rovnaký význam a voľne sa zamieňajú),
- lineárne (riziko ako vyššie štádium hrozby alebo hrozba ako vyššie štádium rizika),
- komplementárne (pojmy sa vzájomne dopĺňajú, realita je vyjadrená prostredníctvom ich totality).

Riziko (grec. *rhiza*) je pojem, ktorý označuje konkrétny jav v mnohých oblastiach života človeka. V najširšom zmysle slova je riziko vnímané ako nebezpečenstvo, strata, možnosť neúspechu.

Riziko býva definované ako určitý druh neistoty, ktoré je možné prostredníctvom štatistických metód kvantifikovať. Vďaka tomu je možné predpovedať vznik nepriaznivých skutočností. Predstavuje tiež označenie možnosti vzniku straty, škody alebo dosiahnutie iného výsledku oproti pôvodne očakávanému, resp. nedosiahnutie očakávaných výsledkov, pričom odchýlky môžu byť buď priaznivé (zisk) alebo nepriaznivé (strata). Riziko však zväčša v sebe skrýva náboj potenciálneho nebezpečenstva nepriaznivého vývoja. (Reitšpís, 2004)

Bezpečnostné riziko podľa Nečasa a Ivančíka (2011) kvantifikuje možnosť prepuknutia neželaného javu. Vyjadruje pravdepodobnosť poškodenia bezpečnostných záujmov identifikova- nou hrozbou. Na stránke Národného bezpečnostného úradu SR (ďalej len „NBÚ“) v Krátkom slovníku hybridných hrozieb riziko predstavuje mieru ohrozenia, ktorá je vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami. (Krátky slovník..., 2022)

Hrozba (ang. *threat*) môžeme v najširšom zmysle slova vnímať ako blízkosť niečoho nebezpečného, rovnako ako aj napomínanie či pohrozenie.

---

aj do štátnej a verejnej správy, a tým aj do oblasti bezpečnosti a obrany. Vedecko-technický a technologický pokrok v oblasti informačných a komunikačných technológií tak prináša nielen nové benefity, príležitosti a výzvy, ale aj viaceré negatíva spojené s novými bezpečnostnými rizikami a hrozbami (Ivančík – Nečas, 2020, s. 47).

Hrozba je podľa § 3 písm. j) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť, to znamená potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí škodu, alebo iný nepriaznivý následok.

Ako uvádza Jurčák a kol. (2017), pojem hrozba sa často nahradzuje slovom ohrozenie, ktorého význam síce v slovníku slovenského jazyka nie je vyjadrený, je to slovo odvodené, ale ktoré sa v rámci odbornej komunikácie používa vo forme prídavného mena s významom – nachádzajúci sa v nebezpečnej, ťažkej situácii, vystavený nebezpečenstvu (náporu, napadnutiu, útoku, ap.), ktorému hrozí inak zánik, skaza, poškodenie. Ale tiež môže mať význam ako ohrozený na živote, ohrozená vlasť, ohrozené mesto, bezpečnosť, nezávislosť, atď.

Novotný (2003) zadefinoval hrozbu ako subjekt, jav či udalosť, ktoré môžu svojim pôsobením poškodiť alebo úplne zničiť chránené hodnotu alebo záujem iného subjektu, pričom hrozba existuje objektívne, nezávisle od konania a vôle objektu, ktorý je ohrozený.

Bezpečnostnú hrozbu Nečas a Ivančík (Nečas, Ivančík, 2011) charakterizujú ako identifikovaný potencionálne deštrukčný a neželaný jav vo vzťahu k bezpečnostným záujmom referenčného subjektu. Takouto hrozbou sa stáva určitý jav v okamihu, keď si príslušný referenčný subjekt uvedomí, že daný jav má potenciál spôsobiť ujmu na jeho bezpečnostných záujmoch. To znamená, že bezpečnostná hrozba vystupuje vždy vo vzťahu k bezpečnostným záujmom referenčného subjektu.

Biela kniha o obrane SR (2016) jednoznačne zadefinovala, aké hrozby budú ovplyvňovať vonkajšie bezpečnostné prostredie SR – hrozby asymetrického charakteru budú prevládať nad hrozbami symetrického charakteru. Z dlhodobého časového horizontu predpokladala ich nárast, rozšírenie spektra a zvýšenie deštruktívnych účinkov, pričom ako je v nej uvedené, nie je možné vylúčiť ani variant, že niektoré asymetrické hrozby môžu postupne eskalovať do hrozieb vojenského charakteru – čo sa aj naplnilo vo februári tohto roku útokom Ruska na Ukrajinu.

Hybridné hrozby nepredstavujú novinku, ktorú by ľudstvo predtým nepoznalo. Práve naopak. Rôzne formy hybridných hrozieb môžeme nájsť naprieč celou históriou ľudstva, pričom môžu byť priame, nepriame alebo latentné. Išlo o rôzne spôsoby ovplyvňovania určitej záujmovej skupiny alebo celej spoločnosti, jej nálad a postojov, alebo o uzatváranie verejne známych ako aj utajených spojeneckých zmlúv a paktov, podplácanie ďalších aktérov konfliktu, atď. Hybridné hrozby predstavovali vždy veľmi silný a účinný nástroj na dosahovanie vlastných cieľov aktérov, aj keď často neboli také „rýchle“ ako priama konfrontácia nepriateľa konvenčnými zbraňami.

2 HYBRIDNÉ HROZBY

Hybridné hrozby môžeme v najširšom zmysle definovať ako súbor rôznorodých (zmiešaných) hrozieb, ktoré spolu vytvárajú kompaktný celok. Zmes nástrojov, metód a prostriedkov, ktoré majú jediný cieľ – ohroziť, zastrašiť alebo eliminovať nepriateľa.

Hoffman (2007) hybridné hrozby definuje ako správanie akéhokoľvek nepriateľa, ktorý súčasne využíva na mieru prispôsobený komplex konvenčných zbraní, neregulárnej taktiky, terorizmu a kriminálneho správania v rovnakom čase a priestore na dosiahnutie svojich politických alebo iných cieľov.

Medzi najefektívnejšie hrozby patria tie, ktoré spôsobia neúmerne vysoké škody vo vzťahu k zdrojom, času a financiám vynaložených útočníkom. V ideálnom prípade by sa účinok asymetrického útoku mohol prejaviť až na strategickej úrovni bez ohľadu na to, na akej úrovni bol realizovaný. (Novotný, 2003)

Zložitosť hybridných hrozieb spočíva v ich komplexnosti, skrytosti a v náročnej preukázateľnosti zo strany napadnutej krajiny, pričom krajina, ktorá hybridné hrozby používa ich popiera. Snaha o riešenie tohto problému je viditeľná a potrebná - napr. v rozšírenej spolupráce členských štátov NATO a EÚ, ktoré sú častými obeťami kybernetických útokov. Obe organizácie pochopili, že možnosť eliminácie hybridných hrozieb a hybridnej vojny je len v úzkej spolupráci, vzájomnej informovanosti a zdieľaní síl a prostriedkov. Už v roku 2016 obidve organizácie definovali spoločné vyhlásenie o implementácii spoločnej deklarácie podpísanej predsedom Európskej rady, predsedom Európskej komisie a generálnym tajomníkom NATO, ktorej obsahom bol boj proti hybridným hrozbám, operačná spolupráca, kybernetická bezpečnosť, obranný priemysel, výskum, budovanie obranných a bezpečnostných kapacít. (Jurčák a kol., 2017)

Hybridné hrozby zadefinoval Glenn (2009) nasledovne – protivník, ktorý súčasne a adaptabilne využíva rôzne kombinácie politických, ekonomických, sociálnych, informačných aktivít a nástrojov moci a zároveň konvenčné, nepravidelné, teroristické a rozvratné kriminálne spôsoby vedenia boja, pričom protivníkom môže byť štátny alebo neštátny aktér, prípadne ich kombinácia.

V Krátkom slovníku hybridných hrozieb NBÚ (2002), je hybridná hrozba zadefinovaná nasledovne - predstavuje súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny. Hybridná hrozba je charakteristická simultánnym použitím viacerých nástrojov koordinovaným spôsobom s cieľom využiť zraniteľnosti (slabé miesta) protivníka a následne oslabiť jeho rozhodovacie procesy pri zachovaní určitého stupňa hodnoverného popretia. Strategickým cieľom týchto hrozieb je oslabenie dôvery verejnosti v demokratické inštitúcie, prehĺbenie nezdravej polarizácie na národnej a medzinárodnej úrovni, spochybnenie základných hodnôt demokratických spoločností, zisk geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných a ovplyvňovania demokratických rozhodovacích procesov.

Medzi „nové“ typy hrozieb, ktoré sú súčasťou hybridných hrozieb radí Jurčák a kol. (2017):

- ***nástroje informačnej vojny*** - akým sú napr. propaganda, antipropaganda. Sú to klasické hybridné hrozby, voči ktorým je veľmi ťažké ubrániť sa. Sú postavené na sociálnej zraniteľnosti a protisystémových náladách v spoločnosti, ktoré sú vyvolávané tzv. trollmi cez internet (troll je anonymný účastník online diskusií, internetových fór, chatov a blogov, ktorý zámerne zasiela provokatívne, urážlivé alebo irelevantné príspevky k citlivým témam s cieľom vyprovokovať ostatných užívateľov k emotívnym odozvám, alebo inak narušiť normálnu vecnú diskusiu).
- ***hrozby súvisiace s kybernetickým priestorom*** - kybernetické útoky, kyberterorizmus, hacktivizmus (spojenie slov hackerstvo a aktivizmus – ide o podvratné používanie počítačov a počítačových sietí s cieľom podporiť politickú propagandu a dosiahnuť politické zmeny),
- ***whistle-blowing*** – v slovenskom ponímaní ide o oznamovateľov protispoločenskej činnosti. V kontexte hybridných hrozieb však za whistle-blowera pokladáme osobu, ktorá vyzradí tajné informácie verejnosti alebo cudzej moci s cieľom dosiahnuť vlastný zisk alebo zabezpečiť konkurenčnú výhodu (príkladom whistle-blowera je napríklad stránka Wikileaks a jej zakladateľ Julian Assange, ktorý zverejnil utajované dokumenty vlády, alebo Edward Snowden, ktorý dal novinárom denníka The Guardian k dispozícii dokumenty o sledovacích aktivitách americkej NSA).
- ***narušanie funkcie kritickej infraštruktúry*** – ide o zariadenia, služby a informačné systémy životne dôležité pre riadenie štátu. Ich narušenie by mohlo mať za následok kolaps fungovania štátu alebo jeho prvkov.

- ***ekonomické a finančné aktivity*** – vzhľadom na globalizáciu a závislosť sveta od ekonomického vývoja a finančných trhov. Cielené pôsobenie v tejto oblasti by mohlo mať za následok až oslabenie obranyschopnosti štátu.
- ***podvratné politické akty*** – sú to akty, ktorých cieľom je narušiť politickú stabilitu štátu a ohroziť tak plnenie funkcií štátu. Nositeľom politických podvratných aktivít sa v súčasnosti stávajú hlavne extrémistické strany a hnutia – subjekty, ktorých cieľom je zmena zriadenia štátu, napr. národno-osloboditeľské hnutia.

Použitie hybridných hrozieb na Slovensku už niekoľko rokov registrujú nielen príslušné autority, ale začína si ich uvedomovať aj verejnosť. Výraznejšie začali uvedené hrozby atakovať SR anexiou Krymu, vypuknutím COVID pandémie, kedy sa výrazne spolarizovala spoločnosť a vrcholí dezinformáciami o napadnutí Ukrajiny Ruskom. Hybridná vojna na našom území už dávno začala a kompetentné orgány v spolupráci s NATO a EÚ sa snažia hľadať efektívne a rýchle riešenia.

3 HYBRIDNÁ VOJNA

Hybridná vojna predstavuje podobne ako hybridné hrozby pojem, ktorý sa v posledných rokoch, a zvlášť po vypuknutí konfliktu na Ukrajine, objavuje čoraz častejšie nielen v slovníku vojakov, vojenských teoretikov alebo bezpečnostných expertov, ale aj v slovníku politikov, novinárov či diskutujúcich občanov (Ivančík, 2016, s. 131).

V najširšom zmysle taký druh vojny, ktorý je charakterizovaný špecifickou kombináciou prostriedkov a metód symetrického a asymetrického charakteru. Súhlasíme so slovami bývalého amerického ministra obrany Roberta M. Gatesa (in Jurčák a kol., 2017), ktorý na margo škály možných hrozieb v rámci príprav vyváženej stratégie Pentagonu na ďalšie obdobie už v roku 2009 uviedol, že v budúcnosti je možné očakávať ešte väčšie množstvo deštrukčných nástrojov a taktiky, od sofistikovaných až po jednoduché, ktoré budú uplatňované v hybridných konfliktoch alebo ešte v komplexnejších formách boja.

Hoffman (2007) vníma hybridnú vojnu ako ten druh vojny, ktorá môže byť vedená nielen štátnymi ale aj neštátnymi aktérmi, pričom v sebe spája rôzne typy vedenia vojny – konvenčné kapacity, neregulárne taktiky a formácie, teroristické aktivity uskutočňované nevyberavým násilím a kriminálnymi nepokojmi.

Hybridná vojna predstavuje viac ako len konflikt medzi štátmi a inými ozbrojenými skupinami. Je aplikáciou rôznych foriem konfliktu, ktoré najlepšie odlišujú hybridné hrozby alebo hybridné konflikty[3].

Hybridná vojna predstavuje podľa Jurčáka a kol. (2017) akt násilia, ktorý je uskutočňovaný s výrazne rozdielnymi prostriedkami alebo spôsobmi, s cieľom donútiť protivníka, aby sa podriadil našej vôli, alebo ako pokračovanie politiky výrazne rozdielnymi prostriedkami, pričom uskutočňovanie politiky sa vykonáva otvorene i skryto, rôznymi aktivitami štátnych i neštátnych aktérov, vojenskými i nevojenskými prostriedkami, konvenčnými i asymetrickými formami vedenia vojny, a to aj bez jej vyhlásenia.

V súčasnosti nie je definované, aký rozsah, intenzitu a efektívnosť činností môže mať hybridná vojna. V prostredí NATO môžeme považovať za oficiálnu definíciu G. Lasconjariasa, J. A. Larsena a kol. (in Jurčák a kol., 2017, s. 28) z NATO Defence College v Ríme, kde je hybridná vojna definovaná ako „*vhodná kombinácia a miešanie rôznych regulárnych a nekonvenčných prostriedkov konfliktu, s dominanciou informácií a riadením médií v rámci fyzického a psychologického bojiska, s používaním všetkých možných*

[3] Tieto rôznorodé aktivity môžu byť vykonávané viacerými samostatnými jednotkami (alebo dokonca tou istou jednotkou), pričom sú operačne a takticky riadené a koordinované v priestore operácie za účelom dosiahnutia synergického efektu vo fyzickom i psychologickom rozmere konfliktu. Želené účinky pritom možno dosiahnuť na všetkých úrovniach konfliktu. (Hoffman, 2007)

prostriedkov pre redukciu svojho odhalenia.“ To môže obsahovať i potrebu dislokovanej tvrdej vojenskej sily, s cieľom zlomiť vôľu protivníka a eliminovať podporu týchto autorít miestnym obyvateľstvom. Jedným z cieľov hybridnej vojny je narušiť silné stránky Aliancie – solidárnosť a vzájomnú dôveru Aliancie. (Jurčák a kol., 2017)

Poprední českí autori Kříž, Schevcuk a Števkov (2015) sa v rámci projektu Jagello 2000 zaoberali hybridnou vojnou ako novým fenoménom v bezpečnostnom prostredí Európy, pričom vytvorili návrh komplexnej definície hybridnej vojny nasledovne – ide o ozbrojený konflikt vedený kombináciou nevojenských a vojenských prostriedkov s cieľom ich synergickým efektom prinútiť protivníka k vykonaniu takých krokov, ktoré by sám o sebe nevykonal. Aspoň jednou stranou konfliktu je štát. Hlavnú úlohu pri dosiahnutí cieľov vojny hrajú nevojenské prostriedky v podobe psychologických operácií a propagandy, ekonomických sankcií, embárg, kriminálnych aktivít, teroristických aktivít a iných subverzívnych aktivít podobného charakteru. Vojenské operácie útočníka sú vedené nepravidelnými silami kombinujúcimi symetrické a asymetrické spôsoby vedenia bojovej činnosti proti celej spoločnosti a najmä proti jej politickým štruktúram, orgánom štátnej správy a samosprávy, ekonomike štátu, morálke obyvateľstva a ozbrojeným silám.

Ako vyplýva z uvedených definícií, aktivity Ruska na území členských štátov NATO a EÚ môžeme oprávnene označiť za hybridné hrozby použité v hybridnej vojne vedenej Ruskom proti členským štátom oboch organizácií. Oveľa zásadnejšiu, dramatickejšiu a „reálnu“ podobu nadobudli hybridné hrozby v spojení s konvenčnými zbraňami v konflikte na Ukrajine, kde sa porušujú ľudská práva, Ženevské konvencie a medzinárodné právo.

Hybridná vojna vďaka výdobytkom vedecko-technického pokroku už dávno získala označenia ako neopakovateľná, flexibilná, „lacná“ cesta zničenia spoločnosti, štátu alebo iného protivníka bez oficiálneho vyhlásenia vojny. Práve tieto atribúty robia hybridnú vojnu takou zaujímavou a zároveň nebezpečnou, nakoľko nepriateľ nemusí byť jednoznačne identifikovateľný, môže sa skrývať a „nenápadne“ vnucovať spoločnosti svoje či už politické, ekonomické alebo sociálne predstavy, ktoré môžu doviesť štát až na pokraj destabilizácie spoločnosti, ohrozenie bezpečnosti alebo izolácii.

Jurčák a kol. (2017) uvádzajú, že hybridná forma vedenia vojny nemá v porovnaní s otvorenou formou vedenia vojny relatívne ustálenú a vopred danú šablónu vykonania a tiež terminológiu. Analýza reálneho použitia hybridných foriem vedenia vojny ukazuje, že je pre ňu charakteristická odlišnosť a neopakovateľnosť usporiadania jej komponentov a prvkov od prípadu k prípadu. Hybridná forma vedenia vojny sa počas vykonávania prispôsobuje zmenám v strategickom a operačnom prostredí. Inými slovami agresor, ktorý používa hybridnú formu vedenia vojny, volí použitie komponentov a ich prvkov (v rámci nich mix nástrojov a prostriedkov) často *ad hoc* podľa jeho aktuálnych možností a vývoja situácie v napadnutej krajine.

Samozrejme, uvedený druh hrozieb nevyužíva voči členskými štátom NATO a EÚ iba Rusko, ale ďalšie štáty z rôznych častí sveta, a to na postupné dosahovanie svojich (zväčša latentných) cieľov. Medzi veľkých „hráčov“ môžeme zaradiť napríklad Čínu, ktorá zásadným spôsobom a cielene zasahuje do vnútorného bezpečnostného prostredia vybraných štátov ako aj do vonkajšieho bezpečnostného prostredia v rámci regiónov ako aj v celosvetovom meradle. Rovnako ako Rusko pôsobí Čína cielene nielen na vojenské, bezpečnostné ciele, ale aj na ekonomické, politické, energetické, sociálne a environmentálne ciele. Hybridná vojna stojí na rozdiel od tej regulárnej (ako môžeme vidieť v Tabuľke č.1) agresora podstatne menej peňazí, vycvičeného a vyzbrojeného personálu, materiálnych zásob a nepotrebuje adekvátne a vierohodne odôvodniť svojim občanom, prečo zaútočil na iný štát.

Tabuľka 1 Vybrané odlišnosti foriem vojny

VYBRANÉ ODLIŠNOSTI FORIEM VOJNY		
KOMPONENTY A AKTIVITY	HYBRIDNÝ SPÔSOB VEDENIA VOJNY	OTVORENÁ/TOTÁLNA VOJNA
Právny stav	Bez vyhlásenia vojny	Vyhlásenie vojny
Aktér vojny	Štát, neštátni aktéri	Štát
Primárny cieľ	Nejasná identifikácia nepriateľa	Jednoznačná identifikácia nepriateľa
Druhy operácií	Vnútenie svojich predstáv o politickom, hospodárskom, zahraničnom vývoji krajiny použitím vojenských i nevojenských prostriedkov	Vnútenie svojich predstáv o politickom vývoji krajiny použitím vojenských prostriedkov
Použité sily	Spravidla asymetrické vedenie operácií	Spravidla symetrické vedenie operácií
Mobilizácia a vojnové hospodárstvo	Kombinácia použitia regulárnych a neregulárnych síl	Regulárne sily
Hlavný objekt záujmu	Obyvateľstvo, využiť jeho protestný potenciál	Štát – ochromiť plnenie funkcií štátu
Hlavné komponenty a aktivity	Asymetrická taktika informačného boja, propaganda a aktivity v kybernetickom priestore	Taktiky a operácie z celého spektra operácií
Miesto	Celé územie štátu	Oblasť záujmu je fyzicky daná a vytýčená, zväčša chránená ozbrojenými silami
Fyzický kontakt bojujúcich strán	Spravidla bez fyzického kontaktu bojujúcich strán	Prevláda fyzický kontakt bojujúcich strán

Zdroj: vlastné spracovanie podľa Jurčák a kol. 2017

Ruský model vníma ľudskú myseľ ako veľké bojisko, na porážku ktorej treba využiť znalosti nielen z vojenskej oblasti, ale aj psychológie, medicíny, biochémie, atď. Toto sociálne inžinierstvo síce nie je novým nástrojom ľudstva na ovládanie nepriateľa. Rôzne techniky boli používané už v staroveku, ale rýchly vývoj v oblasti vedy a techniky umožňuje v sociálnom inžinierstve využívať metódy a prostriedky, ktoré sme doteraz nepoznali, resp. nemali k dispozícii. Práve kvôli efektívnosti a dočasnému nedostatku „protizbraní“ voči aktuálnym hybridným hrozbám majú hybridné vojny taký veľký úspech. Čekinov a Bogdanov (in Jurčák a kol., 2017) už v roku 2013 rozdelili priebeh tzv. „vojny novej generácie“ (hybridnej vojny) do nasledujúcich fáz:

1. nevojenské asymetrické vedenie vojny zahŕňajúce informačné, psychologické, ideologické, diplomatické a ekonomické opatrenia ako časť plánu na vytvorenie priaznivých politických, ekonomických a vojenských predpokladov pre ďalšie fázy vojny,
2. špeciálne operácie s cieľom oklamať politických a vojenských predstaviteľov koordinovanými opatreniami prostredníctvom diplomatických kanálov, masovo-komunikačnými prostriedkami, vládnych a vojenských agentúr, únikom falošných údajov, rozkazov, nariadení a smerníc,
3. zastrašovanie, klamanie, podplácanie vládnych a vojenských predstaviteľov s cieľom prinútiť ich, aby prestali plniť svoje služobné povinnosti,
4. destabilizujúca propaganda, ktorá má zvýšiť nespokojnosť obyvateľstva, čo bude umocnené príjazdom militantných skupín a eskaláciou podvratnej činnosti,

5. zriadenie bezletových zón nad krajinou, ktorá ma byť napadnutá, vyhlásenie blokády a rozsiahle využitie súkromných vojenských spoločností v tesnej spolupráci s ozbrojenými opozičnými jednotkami,
6. zahájenie vojenských akcií, ktorým predchádzal rozsiahli prieskum a diverzná činnosť, t. j. všetky typy, formy a metódy operácií, vrátane operácií špeciálnych jednotiek, operácií vo vesmíre, rádiové a elektronické operácie, diplomatické spravodajstvo, spravodajstvo tajných služieb a priemyslová špionáž,
7. operácie vedené prostredníctvom cielených informácií, elektronický boj, letecké a kozmické operácie, nepretržité letecké zastrašovanie v súčinnosti s použitím vysoko presných zbraňových systémov (vrátane mikrovĺn, radiácie, neletálnych biologických zbraní, atď.),
8. likvidácia zostávajúcich miest odporu a zničenie zvyškov nepriateľských zoskupení prostredníctvom špeciálnych operácií vedených prieskumnými jednotkami, ktoré vyhľadávajú jednotky nepriateľa a hlásia ich súradnice raketovým a delostreleckým jednotkám, paľba s využitím vyspelých zbraní, sústredená na zničenie jednotiek, ktoré kladú odpor, nasadenie výsadkových jednotiek, ktoré obkľúčia posledné body odporu a operácie na vyčistenie terénu prostredníctvom pozemných jednotiek.

Hybridná vojna Ruska proti zvyšku Európy nabrala nový rozmer zaútočením na Ukrajinu. Práve tento neospravedlniteľný akt zásadným spôsobom zmenil pohľad štátov EÚ ako aj NATO na svoju bezpečnosť, na bezpečnosť v regióne i vo svete. Rusko ako tvrdý oponent NATO a EÚ neustále hľadá spôsoby, ako atakovať fungovanie a bezpečnosť členských štátov Európy a USA. Práve hybridná vojna Ruska proti obom organizáciám posilnila ich vzájomné väzby a spoluprácu, čo v konečnom dôsledku malo za následok silnejšiu prepojenosť a spoluprácu pre zaistenie mieru a stability Európy, regiónu i sveta. Invázia Ruska na Ukrajinu spolupatričnosť členských štátov neoslabila, práve naopak. O zásadnej zmene vďaka tejto invázii môžeme hovoriť aj vo vzťahu odhodlania Fínska a Švédska požiadať o ich vstup do NATO.

ZÁVER

Hybridný spôsob boja zásadným spôsobom mení nadstavenie spoločnosti, jej pocit bezpečia a istoty. Obyvatelia Európy ako aj ostatných štátov si začínajú byť vedomí, že sú priamo alebo nepriamo Ruskom ohrozené ich základné životné potreby, čo v takomto rozsahu zažili naposledy počas a po skončení druhej svetovej vojny. Organizácie ako NATO a EÚ si spolu s medzinárodným spoločenstvom tento fakt dobre uvedomujú, a preto sa snažia reflektovať čo najrýchlejšie a adekvátnym spôsobom na vzniknutú situáciu.

Výbor NATO pre konzultácie, riadenie a velenie predstavuje hlavný výbor pre konzultácie o technických a implementačných aspektoch kybernetickej obrany. Centrum excelentnosti kooperatívnej kybernetickej obrany NATO (ďalej len CCDCOE) je akreditované pre NATO podporuje svoje členské štáty a NATO odbornými znalosťami v oblasti kybernetickej obrany.

EÚ považuje problematiku hybridných hrozieb za výzvu súčasného zaistenia bezpečnosti v Európe. Vo svojom dokumente „*Spoločný rámec pre boj proti hybridným hrozbám*“ prináša jednu z najvyčerpávajúcejších definícií hybridných hrozieb –„ ide o rôznorodú zmes činností, ktoré často zahŕňajú konvenčné aj menej konvenčné metódy, ktoré môžu štáty i neštátne subjekty používať koordinovaným spôsobom, pričom nedosahujú stupeň formálne vyhlásenej vojny. Cieľom nie je len spôsobiť priame straty a zneužiť slabé miesta, ale aj destabilizovať spoločnosť a vyprovokovať neistotu, ktorá má ochromiť rozhodovacie procesy. Rozsah opatrení využívaných v hybridnom ťažení môže byť veľmi široký a siaha od kybernetických útokov na kritické informačné systémy cez narúšanie kritických služieb, ako

sú dodávky energií alebo finančné služby až po podkopávanie verejnej dôvery vo vládne inštitúcie, alebo využívanie sociálnej zraniteľnosti“. (Spoločný rámec pre boj proti hybridným vojnám, 2016 in Jurčák a kol., 2017)

Rusko (ako aj iní aktéri) sa snažia permanentnými a stupňujúcimi sa hybridnými útokmi dosiahnuť svoje vlastné ciele na úkor obyvateľov slobodných demokratických spoločností. V prípade Ukrajiny bohužiaľ neostalo iba pri hybridnej vojne odohrávajúcej sa vo virtuálnom priestore a ktorá tam prebieha už niekoľko rokov, ale Rusko napadlo túto slobodnú krajinu aj fyzicky.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

Biela kniha o obrane SR, 2016

GLENN, W., R. 2009. *Thoughts on Hybrid Conflict. online. Small Wars Journal.* [online] [cit. 2022. 4. 03.] Dostupné na: <http://smalwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict>.

HOFFMAN, G. F. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online] [cit. 2022. 4. 03.] Dostupné na: <http://www.pomacinstitute.org./images/stories/publications/potomac_hybrid_ war_010>.

IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 130-156. ISSN 1339 – 2751. [online] Dostupné na: <http://fmv.euba.sk/files/MV_2016_2_130-156_Ivancik.pdf>.

IVANČÍK, R. – NEČAS, P. 2020. Kybernetická moc v kontexte zaisťovania kybernetickej bezpečnosti a obrany na národnej a aliančnej úrovni. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru v Bratislave, 2020, s. 47-58. ISBN 978-80-8040-819-3.

IVANČÍK, R. 2021a. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 32-53. ISSN 1336-9202. [online] Dostupné na: <http://ak.aos.sk/images/repozitar/vr/vr_3_2021/vr_3_2021_3.pdf>.

IVANČÍK, R. 2021b. Útočné kybernetické operácie ako súčasť hybridných hrozieb. In *Trilobit*, 2021, roč. 13, č. 3, 14 s. ISSN 1804-1795. [online]. Dostupné na: <http://trilobit.fai.utb.cz/utocne-kyberneticke-operacie-ako-sucast-hybridnych-hrozieb>.

IVANČÍK, R. 2022. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022. 240 s. ISBN 978-80-7380-873-0.

JURČÁK, V. – JURČÁK, J. 2018. Hybridná vojna – výzva pre NATO. In *Bezpečnostné fórum 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Banská Bystrica : Belianum – vydavateľstvo Univerzity Mateja Bela, 2018, s. 248-254. ISBN 978-80-557-1093-8.

JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Záverečná správa o riešení vedeckého projektu VV-A1. L. Mikuláš: AOS gen. M. R. Štefánika, 2017., 88 s.

Krátky slovník hybridných hrozieb. [online] Dostupné na: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.

KRÍŽ, Z., SCHEVCUK, Z., ŠTEVKOV, P. 2015. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy.* Jagelo, Ostrava 2000, 16 s.

LAML, R. (2008) Vzťah pojmov hrozba a riziko (II). [online] Dostupné na: <http://mepoforum.sk/bezpecnost/terminologia/vztah-pojmov-hrozba-a-riziko-ii-roman>.

NEČAS, P. – IVANČÍK, R. 2011. *Globalizácia, obrana a bezpečnosť*. Liptovský Mikuláš: Akadémia ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši, 2011. 190 s. ISBN 978-80-8040-425-3

NOVOTNÝ, A. 2003. *NATO a medzinárodná bezpečnosť*. Nové Zámky: CROCUS, 2003. 125 s. ISBN 80-88992-65-6

REITŠPÍS, J. a kol. 2004. *Manažérstvo bezpečnostných rizík*. Žilina: EDIS, 2004. 296 s. ISBN 80-8070-328-0

ZÁKON č. 69/2018 z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

PhDr. Róbert TOMÁŠEK
študent 4. roč. doktorandského štúdia BOŠ
Akadémia ozbrojených síl gen. M. R. Štefánika v L. Mikuláši
roberttomasek.tomasek@gmail.com

Vydavateľ / Publisher: Akadémia ozbrojených síl generála M. R. Štefánika
Editor / Editor: Ing. Daniel BREZINA, PhD.
Dizajn / Graphic design: Mgr. Robert KANDRIK
Počet strán / Number of pages: 329
Náklad / Edition: online
Vydané / Published: 2022
Uverejnené príspevky v zborníku neprešli jazykovou korektúrou.
Published papers in the proceedings did not undergo language correction.
Za obsahovú stránku, odbornú a jazykovú úroveň zodpovedajú v plnom rozsahu autori príspevkov.
The content and the professional and language levels of the papers are in the full responsibility of the authors.
ISBN 978-80-8040-631-8