DOI: https://doi.org/10.52651/vr.a.2025.2.70-86

VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Číslo 2, Strana 70-86

ZRANITEĽNOSŤ SOCIÁLNYCH SYSTÉMOV V KONTEXTE KYBERNETICKÝCH HROZIEB

Roman Bartolomej BOROVSKÝ

THE VULNERABILITY OF SOCIAL SYSTEMS IN THE CONTEXT OF CYBER THREATS

HISTÓRIA ČLÁNKU

Doručený: *23.09.2025*
Schválený: *27.11.2025*
Vydaný: *31.12.2025*

ABSTRACT

The article explores the link between social systems and cybersecurity, analyzing interactions between technology, social structures, and security threats. It examines cyber threats from technological, psychological, and organizational perspectives and analyzes real-world attacks highlighting cybersecurity's growing geopolitical and economic significance. The author emphasizes that effective protection requires not only advanced technology and regulations but also user awareness. The conclusion stresses the need for an integrated approach, considering security, social, legal, and economic factors, offering a comprehensive view of cybersecurity in social systems.

KEYWORDS

social systems, cybersecurity, cyberattacks, social engineering

ÚVOD

V kontexte exponenciálne rastúcej digitalizácie sociálnych systémov sa ich štruktúra a dynamika stávajú stále komplexnejšími, pričom interakcia medzi sociálnymi a technologickými prvkami vytvára nové paradigmatické výzvy. Digitálne prostredie v ostatných rokoch preniklo do všetkých sfér spoločenského života, redefinujúc základné vzorce sociálnych interakcií a organizačných štruktúr. Vznikajúce sociotechnické systémy predstavujú symbiotické prepojenie medzi technologickými inováciami a spoločenskými normami, pričom ich bezpečnosť a stabilita sa čoraz viac dostávajú do centra akademického diskurzu.

Článok sa zaoberá skúmaním charakteristík sociálnych systémov, pričom osobitnú pozornosť venuje ich interakcii s kybernetickou bezpečnosťou a sociálnym inžinierstvom. Cieľom autora je konceptuálne uchopiť sociotechnickú dynamiku v kontexte kybernetických hrozieb a manipulácie, a zároveň identifikovať praktické implikácie týchto fenoménov pre jednotlivcov i organizácie. Výskumný rámec zahŕňa teoretickú reflexiu na základe

relevantných sociologických a technologických prístupov, ako aj prípadové štúdie kybernetických incidentov z holistickej perspektívy.

Prvá časť článku sa sústreďuje na definovanie základných koncepčných rámcov sociálnych systémov, pričom vychádza zo sociologických teórií o ich štruktúre a fungovaní. Následne je analyzovaná vzájomná interdependencia medzi technologickými inováciami a sociálnymi entitami, pričom sa reflektuje úloha kybernetickej bezpečnosti v ochrane týchto systémov. Osobitná pozornosť je venovaná fenoménu sociálneho inžinierstva ako jednej z najefektívnejších foriem kybernetických útokov, využívajúcej psychologické a behaviorálne slabiny používateľov informačných technológií.

Na základe syntézy teoretických poznatkov a analýzy konkrétnych kybernetických incidentov autor identifikuje kľúčové faktory ovplyvňujúce odolnosť sociotechnických systémov voči digitálnym hrozbám. Osobitne hodnotí efektívnosť aktuálnych bezpečnostných opatrení a zdôrazňuje potrebu multidisciplinárneho prístupu pri formulovaní stratégií na prevenciu a mitigáciu rizík.

Problematika skúmaná v tomto článku je vysoko relevantná v kontexte súčasných spoločensko-technologických trendov, keďže kybernetické hrozby predstavujú signifikantný destabilizačný faktor nielen pre informačné systémy, ale aj pre širšie sociálno-ekonomické štruktúry. Hĺbkové pochopenie týchto javov umožňuje formulovať efektívnejšie bezpečnostné stratégie, čím sa vytvára priestor pre budovanie odolnejších a adaptabilnejších socio-technických systémov v ére exponenciálne sa meniaceho digitálneho prostredia.

1 CHARAKTERISTIKA SOCIÁLNYCH SYSTÉMOV

1.1 Terminologické vymedzenie pojmov

Skôr než prejdeme k samotnej podstate tohto článku, zadefinujeme si základné pojmy vzťahujúce sa k danej tematike, pričom sa odvolávame najmä na poznatky zo sociológie. Sociálne skupiny predstavujú základné stavebné kamene sociálnych systémov. Sú tvorené jednotlivcami spojenými spoločnými cieľmi, hodnotami alebo interakciami. Tieto skupiny zohrávajú kľúčovú úlohu v dynamike systému, pričom ich koherencia a odolnosť priamo ovplyvňujú stabilitu celého systému. Pri narušení dôvery alebo integrity v rámci sociálnych skupín, napríklad v dôsledku dezinformačných kampaní, dochádza k fragmentácii a neželaným dopadom na spoločnosť.

Martinská pripisuje sociálnej skupine schopnosť vyjadrovať pospolitosť dvoch alebo viacerých osôb, ktoré majú isté spoločné ciele, vytvárajú spoločné normy a vzájomnú súvislosť sociálnych rolí a považuje ju za kvalitatívne ucelený sociálny útvar, ktorý sa odlišuje kvalitou od iných útvarov. Sociálne skupiny sú integrované zoskupenia, tvoria základnú jednotku spoločenskej štruktúry a ich existencia je kľúčová pre udržanie sociálnej stability. Ich vplyv presahuje individuálnu úroveň, pretože zabezpečujú kontinuálne fungovanie spoločnosti

prostredníctvom sociálnych noriem, hodnôt a pravidiel správania (Martinská, 2019, s. 47).

Sociálna štruktúra v sociológii vyjadruje usporiadanosť sociálneho života vo všeobecnej rovine a usporiadanosť jednotlivých sociálnych zoskupení. Najčastejšie je chápaná ako sieť alebo sústava vzťahov, ktoré spájajú jednotlivé časti spoločnosti do celku. Sociálna štruktúra predstavuje relatívne stabilný súbor sociálnych interakcií a vzťahov medzi ľuďmi v sociálnych skupinách i celej spoločnosti. Tento súbor interakcií prebieha podľa určitých vzorcov a pravidiel, ktoré sú základom organizácie spoločnosti. Stabilita sociálnej štruktúry je dôležitá pre koordináciu spoločenských procesov, zabezpečenie sociálnej harmónie a efektívneho fungovania systémov na rôznych úrovniach (Ibid.).

1.2 Sociálne systémy ako komplexné zoskupenia

Sociálne skupiny sa podieľajú na vytváraní zoskupení vyšších sociálnych systémov. Tvoria ich subsystémy, ktoré fungujú ako osobité samostatné celky. Systém možno vymedziť ako celok, pozostávajúci zo systematicky a navzájom závisle usporiadaných prvkov. Tieto prvky interagujú prostredníctvom procesov, ktoré sú previazané vnútornými väzbami systému, prevažujúcimi nad vonkajšími vplyvmi. Sociálne systémy disponujú vlastnou schopnosťou autopoézie, teda seba vývoja a adaptácie na prostredie (Lourenço, 2010, s. 3).

Podľa Parsonsa má spoločnosť štyri hlavné podsystémy: ekonomický, politický, sociálny a kultúrny. Ekonomický subsystém zabezpečuje statky a zdroje pre rozvoj spoločnosti, politický subsystém sa sústreďuje na „vládnutie“, sociálny subsystém na normy a hodnoty a kultúrny subsystém podporuje spoločenské vzory a hodnoty. Tieto subsystémy realizujú výmenu zdrojov a angažujú sa v dosahovaní spoločných cieľov (In: Šubrt, 2016).

Luhmann chápe sociálne systémy ako uzavreté celky, ktorých vlastnosti sú definované ich vnútornými procesmi. Tieto systémy sú schopné sebareprodukcie a používajú vlastné komunikačné kódy, ktoré sú neprenosné na iné subsystémy. Luhmann zdôrazňuje, že sociálne systémy formujú svoje vlastné štruktúry prostredníctvom výberu a interakcie, pričom ich schopnosť adaptácie umožňuje prežiť v podmienkach neurčitosti a rizika (Luhmann, 1995).

V tomto kontexte je dôležité chápať sociálne skupiny ako základný prvok, z ktorého sa formujú väčšie a zložitejšie sociálne systémy. Rola týchto skupín a ich interakcií ovplyvňuje stabilitu celej sociálnej štruktúry, a tým aj funkčnosť a udržateľnosť spoločnosti ako celku (Matis a Maciejewski, 2017, s. 14).

1.3 Sociotechnické systémy a kybernetická bezpečnosť

Kybernetická bezpečnosť je dnes už neoddeliteľnou súčasťou celého súboru opatrení prijímaných na zaistenie individuálnej aj skupinovej bezpečnosti, resp. opatrení zameraných na zaistenie bezpečnosti na národnej i medzinárodnej úrovni. Predstavuje systém opatrení, technológií a postupov určených na ochranu digitálnych systémov, sietí a dát pred

kybernetickými hrozbami, pričom zahŕňa prevenciu, detekciu a reakciu na bezpečnostné incidenty s cieľom zachovať dôvernosť, integritu a dostupnosť informácií v digitálnom prostredí (Ivančík, 2012).

Kybernetická bezpečnosť sa často redukuje na technické riešenia, ako sú firewally, šifrovanie dát, antivírusové programy a pravidelné aktualizácie softvéru. Hoci tieto opatrenia predstavujú dôležitý pilier ochrany, samotné technológie nestačia na zabezpečenie komplexnej kybernetickej odolnosti. Kľúčovým faktorom, ktorý je často prehliadaný, je ľudský prvok a spôsob, akým jednotlivci a organizácie interagujú s technologickými systémami. V tomto kontexte je potrebné vnímať kybernetickú bezpečnosť nie ako čisto technologický problém, ale ako komplexný systém, v ktorom sa prelínajú technológie, sociálne štruktúry, bezpečnostné a organizačné procesy a správanie používateľov.

Moderné spoločnosti sú charakteristické rastúcou vzájomnou závislosťou medzi ľuďmi a digitálnymi technológiami, pričom tento vzťah je obojstranný – technológie ovplyvňujú spôsob, akým ľudia komunikujú, pracujú a rozhodujú sa, zatiaľ čo ľudské správanie spätne formuje bezpečnostné hrozby a riziká a potrebu obrany a ochrany. Ako uvádza Cavelty, kybernetický priestor možno chápať ako sociotechnický systém, kde technologické inovácie a sociálne praktiky neexistujú oddelene, ale sú v neustálej interakcii. Tento pohľad zdôrazňuje, že akékoľvek bezpečnostné opatrenia musia byť navrhnuté s ohľadom na ľudské správanie a organizačnú dynamiku (Cavelty, 2023, s. 801).

Príkladom tejto závislosti je automatizácia zdravotníckych záznamov, ktorá výrazne zvyšuje efektivitu poskytovania zdravotnej starostlivosti a zrýchľuje prístup k dôležitým informáciám. Zároveň však vytvára nové bezpečnostné riziká, keďže úspešnosť ochrany týchto údajov závisí nielen od technických opatrení, ale aj od správania zdravotníckeho personálu. Ak zamestnanci nedodržiavajú bezpečnostné protokoly, opakovane používajú slabé heslá alebo nevedome poskytujú prístup neoprávneným osobám, môže dôjsť k únikom citlivých údajov, čo môže mať vážne nepriaznivé dôsledky nielen pre pacientov, ale aj pre dôveryhodnosť celého systému.

Sociotechnický subsystém kybernetickej bezpečnosti nie je statická štruktúra, ale dynamické prostredie, ktoré sa neustále prispôsobuje vývoju technológií a meniacim sa útočným metódam. Zatiaľ čo technické prvky, ako sú kryptografické mechanizmy a sieťová bezpečnosť, tvoria základnú ochranu, kľúčovým faktorom úspechu týchto opatrení je stále človek. Používatelia môžu bezpečnostné politiky obchádzať, či už nevedomky alebo úmyselne, čím oslabujú účinnosť inak vysoko efektívnych technologických riešení. Preto je nevyhnutné, aby bezpečnostné stratégie nezahŕňali len vývoj pokročilejších technológií, ale aj pochopenie a riadenie ľudského správania v digitálnom prostredí (Bada et. al., 2015, s. 121-123).

Z toho vyplýva, že efektívne zaistenie kybernetickej bezpečnosti závisí na synergii medzi technológiami a ľudským faktorom. Bez ohľadu na to, aké pokročilé bezpečnostné opatrenia sú implementované, ich účinnosť bude vždy závisieť od správne nastavených

sociálnych a organizačných mechanizmov, ktoré zabezpečia zodpovedné a bezpečné používanie technológií. Kybernetická bezpečnosť v rámci sociálnych systémov preto vyžaduje holistický prístup, ktorý integruje technické riešenia, ľudské správanie a organizačnú dynamiku do jedného súdržného rámca, čo prispieva k vytvoreniu odolnejšej a bezpečnejšej digitálnej infraštruktúry pre budúcnosť.

2 SOCIÁLNE INŽINIERSTVO A KYBERNETICKÉ ÚTOKY

Sociálne inžinierstvo predstavuje psychologickú manipuláciu, pri ktorej útočníci zneužívajú dôverčivosť, nedostatok technického vzdelania alebo sociálne tlaky, aby oklamali používateľov a získali prístup k citlivým údajom či systémom. Na rozdiel od tradičných kybernetických útokov, ktoré sa spoliehajú na technické exploity, sociálne inžinierstvo útočí na ľudský faktor, ktorý je často najslabším článkom bezpečnostných opatrení (Bobokulov, 2023, s. 2-3).

Najväčšia hrozba sociálneho inžinierstva spočíva v tom, že ani najlepšie technologické zabezpečenia nedokážu zabrániť útoku, ak sa používateľ rozhodne dôverovať podvodníkovi. Útočníci často využívajú emocionálne manipulácie, ako sú strach, naliehavosť alebo zvedavosť, čím zvyšujú pravdepodobnosť, že obeť vykoná požadovanú akciu, napríklad poskytne heslo alebo otvorí škodlivý súbor. Tento spôsob útoku je extrémne efektívny, pretože obchádza technické bariéry a zameriava sa na ľudské správanie.

Podľa Choiho a Rubina tvoria útoky v rámci sociálneho inžinierstva viac ako dve tretiny všetkých kybernetických incidentov. Medzi najčastejšie metódy patria:

a) Phishing (77 % všetkých útokov) – Útočník posiela falošné e-maily alebo vytvára podvodné webové stránky, ktoré sa vydávajú za legitímne inštitúcie (napr. banky, vlády, zamestnávateľov). Cieľom je získať prihlasovacie údaje alebo infikovať zariadenie škodlivým softvérom.
b) Vishing (voice phishing) a impersonácia (zosobnenie) – Podvodné telefonáty alebo osobná manipulácia, pri ktorej útočník predstiera, že je zamestnanec technickej podpory, polícia alebo banka, aby vylákal citlivé údaje od obete.
c) Smishing (SMS phishing) – Obeť dostane podvodné SMS správy s odkazmi na škodlivý obsah, ktoré ju môžu presmerovať na falošné stránky alebo ju presvedčia, aby stiahla malvér.
d) Scareware – Útočník vystraší obeť falošnými bezpečnostnými upozorneniami (napr. „Váš počítač je infikovaný! Stiahnite si tento bezpečnostný nástroj.“), čím ju prinúti nainštalovať škodlivý softvér.
e) Pokročilé podvody – Napríklad Business Email Compromise (BEC), pri ktorom útočníci zneužívajú e-mailové účty zamestnancov na falošné finančné transakcie, pričom firmy môžu prísť o tisíce až milióny dolárov (Choi a Rubin, 2023).

Tieto metódy sú vysoko prispôsobivé a využívajú regionálne špecifiká, čím sa stávajú

ešte nebezpečnejšími. Mba a kol. upozorňujú na podvody typu „advance-fee frau“ (podvody s poplatkom vopred) v Nigérii, kde útočníci zneužívajú ekonomickú nestabilitu a manipulujú zraniteľné skupiny, ako sú študenti, nezamestnaní mladí ľudia a ďalšie marginalizované vrstvy spoločnosti. Tieto podvody fungujú na princípe vylákania poplatkov vopred za služby alebo výhody, ktoré nikdy nie sú poskytnuté (Mba, et al., 2017, s. 1301-1307).

Podľa výskumu sa tieto podvody postupne vyvinuli od klasických podvodných listov a telefonátov až po sofistikované online schémy, využívajúce sociálne siete, diskusné fóra a anonymné internetové platformy na oslovovanie obetí. Špecifickým znakom týchto podvodov je ich prispôsobenie sa miestnemu sociálno-ekonomickému prostrediu, pričom útočníci využívajú vysokú nezamestnanosť a nedostatok príležitostí ako nástroj manipulácie (Mba a kol., 2017, s. 1308)

Ľudia prirodzene dôverujú iným ľuďom, technológiám, zariadeniam a inštitúciám, pretože veria v ich zodpovednosť, spoľahlivosť, dobré úmysly či osvedčené fungovanie. Táto dôvera je spravidla výsledkom skúseností, spoločenských noriem a osobných presvedčení. Zvyčajne to platí až dovtedy, kým sa nestanú obeťami podvodu, zneužitia alebo manipulácie (Ivančík, 2022). Útočníci vedia, že ľudia majú tendenciu pomáhať, dôverovať a vyhýbať sa konfliktom, a práve tieto faktory využívajú. Jednoduché techniky môžu obísť aj robustné bezpečnostné systémy, ak útočník presvedčí osobu, aby sama vykonala kompromitujúcu akciu.

Jednou z najnovších foriem sociálneho inžinierstva sú „semantic attacks“ – útoky neútočiace priamo na technológiu, ale manipulujúce vizuálne a obsahové prvky systémov s cieľom oklamať používateľov. Príkladom je webstránka, ktorá vyzerá úplne legitímne, ale v skutočnosti ide o podvodnú kópiu, zhromažďujúcu prihlasovacie údaje.

Kľúčovým aspektom je ľudská zraniteľnosť. Györffy et al. upozorňujú, že aj napriek technickým auditom a školeniam hlavným slabým článkom zostáva nedostatočné povedomie používateľov. Napríklad maďarská štúdia ukázala, že 70 % zamestnancov podceňuje riziká phishingových útokov, pričom len po simulačných cvičeniach (napr. fake phishingové e-maily) sa ich náchylnosť znížila o 20 % (Györffy, et al., 2017, s. 412).

Sociálne inžinierstvo má najväčší dopad na zraniteľné skupiny obyvateľstva, ktoré majú obmedzený prístup k digitálnemu vzdelaniu a skúsenostiam s kybernetickými hrozbami. Seniori sú častým terčom kybernetických podvodníkov, čo potvrdzujú viaceré oficiálne zdroje. Senátny výbor pre starších občanov USA vo svojich zisteniach identifikoval dominantné typy podvodov, ktoré sa zameriavajú na dôverčivosť a slabšiu digitálnu gramotnosť staršej populácie (U.S. Senate, 2016).

Podvodníci v podstate neustále prispôsobujú svoje podvodné taktiky novým trendom a zmenám v legislatíve. V posledných rokoch sa čoraz častejšie objavovali podvody vydávajúce sa za pracovníkov Sociálnej poisťovne, ktorí seniorov zastrašovali údajnými problémami s ich dôchodkom alebo sociálnymi dávkami (U.S. Senate, 2016). Ďalším rastúcim trendom sa stali

„romantické podvody“, ktoré v roku 2020 spôsobili straty vo výške 84 miliónov USD (Federal Trade Commission, 2020). Pri týchto podvodoch útočníci využívajú osamelosť seniorov, nadväzujú s nimi falošné romantické vzťahy a následne ich žiadali o finančnú pomoc pod rôznymi zámienkami.

Tieto prípady poukazujú na neustály vývoj kybernetických hrozieb a zdôrazňujú potrebu nepretržitého vzdelávania a zvyšovania povedomia seniorov, aby sa dokázali efektívne chrániť pred podvodmi v digitálnom prostredí.

2.1 Klasifikácia a rozbor kybernetických útokov

V prípade úspešného útoku v kybernetickom priestore môže byť narušený riadny chod či už verejných alebo súkromných, resp. civilných alebo vojenských zariadení s rozsiahlymi následkami (Jurčák a kol., 2023). Následky takýchto útokov môžu spočívať napríklad v narušení zásobovania širokého spektra zákazníkov, odberateľov, prerušení dodávok energií, výpadkoch výroby v továrňach a v rôznych nevýrobných prevádzkach, taktiež v riadení premávky na letiskách, železniciach, pozemných komunikáciách, narušení fungovania bánk, nemocníc, úradov a pod. Môže tak dochádzať k finančným, materiálnym či časovým stratám alebo v horších prípadoch k ujmám na zdraví alebo dokonca k stratám na životoch (Ivančík, 2021).

Pre označenie páchateľa takýchto útokov sa obyčajne používa anglický termín „hacker“, ktorý vznikol v päťdesiatych rokoch 20. storočia v komunite rádioamatérov. Podľa Jirovského, pojem hacker charakterizoval šikovného a technicky nadaného jedinca schopného hľadať nové spojenia a metódy na zlepšenie výkonu a dosahu svojho vysielača. Počiatkom 70. rokov 20. storočia termín zdomácnel v dnešnom slova zmysle, keď technologickí nadšenci začali zneužívať nedostatočné zabezpečenie telefónnej siete ku nespoplatneným diaľkovým hovorom (Jirovský, 2007, s. 47).

Kybernetická kriminalita vo všeobecnosti má rôzny pôvod a príčinu. Stručne možno poznamenať, že rozlišujeme jednoduché útoky hackerov na málo zabezpečené subjekty (domácnosti a jednotlivci) a rafinované, oveľa zložitejšie útoky, ktoré cielene prelomia aj pokročilé zabezpečenie väčších, súkromných alebo verejných inštitúcií. Keďže sa kybernetické zločiny objavili vo viacerých podobách, v súčasnosti možno zjednodušene identifikovať nasledujúce druhy kybernetickej kriminality:

a) drobní hackeri – ich cieľom je získať prospech predajom ukradnutých dát alebo duševného vlastníctva. Ide o najbežnejšiu formu kybernetickej kriminality;
b) tzv. „hacktivisti“ – hackeri, ktorí útočia na oficiálne kontá inštitúcií s cieľom poukázať na ich slabú ochranu; charakterizuje ich výrazne menšia nebezpečnosť ako v prípade nižšie uvedených druhov. Do tejto kategórie spadajú aj aktivisti využívajúci kybernetické prostriedky na dosiahnutie ideologických, politických, náboženských alebo nacionalistických cieľov (Schmitt, 2017, s. 565).
c) organizovaná kybernetická kriminalita – charakterizuje ju vysoká pokročilosť

a rafinované taktiky na prelomenie zabezpečených sietí. Cieľom je obyčajne získať majetkový prospech značného rozsahu;

d) kybernetický terorizmus – táto forma terorizmu sa radí medzi konvenčné formy neletálneho terorizmu (Jirovský, 2007, s. 129). Útoky sú zamerané proti počítačom, počítačovým sieťam a informáciám v nich uložených s cieľom zastrašiť alebo donútiť vládu alebo obyvateľstvo ku podpore sociálnych alebo politických cieľov teroristickej skupiny (Janoušek, 2007, s. 60). Faktom zostáva, že kybernetický terorizmus je iba podmnožinou terorizmu s rovnakými trestnoprávnymi následkami.

Za útokmi v kybernetickom prostredí stoja častokrát aj samotné štáty sledujúc svoje geopolitické záujmy ako tomu bolo napr. v prípade gruzínsko-ruského konfliktu v roku 2008, kedy bola ruskými hackermi napadnutá dôležitá sieťová infraštruktúra Gruzínska (Tikk, a kol., 2010).

Taktiež samotné zbrojné systémy sú v súčasnosti závislé na informačno-komunikačných technológiách, čo obsahuje veľké riziko zneužitia v prípade nedostatočnej ochrany proti potencionálnym kybernetickým útokom. Vzhľadom na narastajúce kybernetické hrozby vlády po celom svete výrazne zvyšujú svoje rozpočty na kybernetickú bezpečnosť. V USA pre fiškálny rok 2025 Ministerstvo obrany žiada 14,5 miliárd dolárov na kybernetické aktivity, čo predstavuje nárast o 1 miliardu oproti predchádzajúcemu roku. Okrem toho ďalšie civilné americké agentúry majú rozpočet 13 miliárd dolárov na kybernetickú bezpečnosť, pričom Agentúra pre kybernetickú bezpečnosť a infraštruktúrnu bezpečnosť (CISA) má pridelené 3 miliardy dolárov (Doubleday, 2024).

Európska únia sa rozhodla reagovať na škodlivé kybernetické činnosti aj legislatívnou cestou s cieľom posilniť svoje spôsobilosti na boj proti nim. Rozhodnutím rady (SZBP) 2019/797 umožnila prijímať cielené reštriktívne opatrenia sledujúc zámer odstrašiť a odradiť potenciálnych útočníkov, zároveň však ponechávajúc každému členskému štátu *„možnosť prijať vlastné rozhodnutie o priznaní zodpovednosti za kybernetické útoky tretiemu štátu“* (EÚ, 2019, čl. 1, ods. 9). Medzi tieto kybernetické útoky patria aj útoky so závažným vplyvom na krajiny mimo EÚ alebo na medzinárodné organizácie, ak sa kroky považujú za potrebné na dosiahnutie cieľov spoločnej zahraničnej a bezpečnostnej politiky EÚ v súlade s čl. 21 ZEÚ (EÚ, 2019, čl. 1, ods. 6).

Kybernetické útoky, ktoré patria pod dikciu nového sankčného režimu, zahŕňajú útoky na informačné systémy patriace do:

a) kritickej infraštruktúry nevyhnutnej pre základné funkcie spoločnosti alebo zdravia, ochrany, bezpečnosti a kvality života obyvateľov z ekonomického alebo sociálneho hľadiska,
b) služieb nevyhnutných na zachovanie základných spoločenských a hospodárskych činností, najmä v oblasti energetiky, dopravy, bankovníctva, financií, zdravotníctva, pitnej vody, digitálnej infraštruktúry,
c) kritických funkcií štátu, najmä v oblasti obrany, riadenia a fungovania inštitúcií, volieb do

verejných funkcií, hospodárskej a občianskej infraštruktúry, vnútornej bezpečnosti a zahraničných vzťahov vrátane diplomatických misií,

d) uchovávania utajovaných skutočností alebo manipulovania s nimi alebo
e) tímov reakcie na núdzové situácie, ktoré sú súčasťou verejnej správy.

Kybernetické útoky realizované štátmi sú veľkou výzvou aj pre medzinárodné právo verejné, nakoľko neexistujú pevné výkladové pravidlá noriem pochádzajúcich častokrát ešte z minulého storočia.

V literatúre sa často skloňujú aj ďalšie slovné spojenia označujúce nežiadúce činnosti aktérov v kybernetickom priestore ako napríklad kybernetické metódy (alternatívne „prostriedky“) vedenia vojny alebo kybernetické operácie. Z pohľadu medzinárodného práva ozbrojeného konfliktu je však diferenciácia zbytočná, nakoľko každá forma vedenia vojny spadá pod jeho princípy (Medzinárodný súdny dvor, 1996).

Slovné spojenie „kybernetické operácie“ je vnímané ako najširší pojem a zahŕňa akúkoľvek aktivitu v kybernetickom priestore, ktorá sa zameriava na dosiahnutie cieľov v rámci kybernetického priestoru alebo prostredníctvom neho (Dinstein, 2020, s. 19).

Z pohľadu práva ozbrojeného konfliktu je vypátranie pôvodcu počítačového vírusu esenciálnou záležitosťou, nakoľko jeho normám podliehajú iba subjekty konajúce v mene štátu a nie jednotlivcov, či skupín. Skupina uznávaných právnych odborníkov sa však zhoduje na skutočnosti, že kybernetické operácie majú potenciál nadobudnúť atribút medzinárodného ozbrojeného konfliktu so všetkými medzinárodnoprávnymi dôsledkami (ICRC, 2016, s. 997-998).

2.2 Kybernetické útoky „Petya“ a „NotPetya“

Rada Európskej únie prijala 24. júna 2024 rozhodnutie (SZBP) 2024/1779, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty. Toto rozhodnutie rozširuje zoznam osôb podliehajúcich reštriktívnym opatreniam o šesť jednotlivcov zodpovedných za významné kybernetické útoky predstavujúce externú hrozbu pre Úniu alebo jej členské štáty. Medzi týmito osobami sú členovia skupín ako „Callisto“ a „Armageddon“, ktoré sú spájané s ruskými vojenskými a spravodajskými službami a sú zodpovedné za sofistikované phishingové kampane a útoky na kritickú infraštruktúru. Rozhodnutie zdôrazňuje rastúcu hrozbu kybernetických útokov, najmä v súvislosti s nevyprovokovanou agresiou Ruska voči Ukrajine, a potrebu koordinovanej reakcie Únie na tieto hrozby.

Prijaté opatrenia nadväzujú na predchádzajúce sankcie, ktoré Rada EÚ zaviedla už v polovici roka 2020 na základe rozhodnutia 2019/797. Vtedy po prvýkrát uložila reštriktívne opatrenia voči šiestim fyzickým osobám a trom právnickým subjektom, ktoré sa podieľali na závažných kybernetických útokoch. Medzi nich patrili pokus o kybernetický útok na Organizáciu pre zákaz chemických zbraní (OPCW) a útoky verejnosti známe pod názvami

„WannaCry“, „NotPetya“ či „Operation Cloud Hopper“. V rámci týchto sankcií EÚ uložila zákaz cestovania do krajín Únie, obmedzenie obchodných aktivít a zmrazenie finančných aktív útočníkov.

Tieto opatrenia sú súčasťou širšej stratégie EÚ na posilnenie kybernetickej bezpečnosti a odstrašenie aktérov, ktorí vykonávajú deštruktívne kybernetické operácie proti jej inštitúciám a členským štátom.

Z pohľadu medzinárodného práva najzaujímavejším postihnutým subjektom je Hlavné stredisko pre špeciálne technológie hlavného riaditeľstva generálneho štábu ozbrojených síl Ruskej federácie (ďalej ako „GTsST“). Podľa Rozhodnutia Rady bolo GTsST zodpovedné za kybernetické útoky s významným dopadom na EÚ a tretie štáty pochádzajúcim z krajiny mimo územia Únie, vrátane kybernetických malvérových útokov známych pod menom „EternalPetya“ alebo „NotPetya“ uskutočnených v júli roku 2017, ako aj skorších kybernetických útokov namierených voči ukrajinskej elektrickej rozvodňovej siete v rokoch 2015 a 2016. GTsST sa podľa Rady EÚ aktívne podieľalo na vyššie spomenutých kybernetických činnostiach a môže byť napojené na útočníkov (EÚ, 2020.

Pôvodná iterácia ransomvéru „Petya“ bola identifikovaná v marci 2016 a šírila sa prostredníctvom emailovej komunikácie obsahujúcej dve prílohy, ktoré predstierali, že ide o dokumenty spojené so žiadosťou o zamestnanie. Jednalo sa o sofistikovanú kombináciu sociálneho inžinierstva a malvéru, pričom jedna z príloh bola neškodne vyzerajúci obrazový súbor a druhá prezentovaná ako životopis vo formáte PDF, v skutočnosti obsahovala spustiteľný kód. Po jeho aktivácii sa vykonal neautorizovaný reštart zariadenia a ransomvér nahradil pôvodný bootloader Windows vlastnou verziou, čo viedlo k strate prístupu k disku.[1] Na rozdiel od tradičných ransomvérových modelov, Petya nezašifroval jednotlivé súbory, ale efektívne zablokoval celý disk, čím eliminoval možnosť obídenia malvéru jednoduchou obnovou dát. Ransomvér Petya vyžadoval od užívateľov zaplatenie výkupného v kryptomene Bitcoin, s priemernými požadovanými sumami v rozmedzí niekoľko stoviek až tisícok dolárov (Pacquet – Clouston, 2019).

O pár mesiacov neskôr, v júni 2017 sa kybernetickým priestorom začala šíriť nová verzia malvéru, ktorá infikovala počítačové siete primárne na Ukrajine, ale zasiahla aj ďalšie európske krajiny. Nový variant nepotreboval žiadnu súčinnosť používateľa, šíril sa samostatne a páchal oveľa väčšie škody. Známa technologická firma Kaspersky Lab po jeho preskúmaní potvrdila, že sa nejedná o predchádzajúcu verziu ransomvér Petya a pomenovala ho príznačne „NotPetya“ (Kaspersky, 2017).

„Wiper útoky“ a ransomvér majú na prvý pohľad podobný priebeh – oba typy malvéru napadnú systém, zašifrujú alebo zmenia dáta a často zobrazia výzvu na zaplatenie výkupného. Kľúčový rozdiel však spočíva v zámere útočníkov. Pri ransomvérovom útoku je hlavným cieľom finančný zisk – útočníci ponúkajú možnosť obnovy dát po zaplatení výkupného, hoci to nie

[1] Petya napáda iba operačné systémy typu Windows – pozn. autora

vždy garantujú. Naopak, wiper útoky sú čisto deštruktívne, pričom ich účelom nie je vydieranie, ale nenávratné poškodenie dát. Práve tento princíp sa naplno prejavil pri útoku NotPetya, kde sa pôvodný zámer ransomvéru Petya – získať od napadnutého používateľa peniaze – zmenil na zámer úplne zničiť dáta bez možnosti obnovy. Radikálny nárast efektivity oproti pôvodnej verzii mohol byť uskutočnený vďaka modifikácii kódu a zapojeniu štátnych kybernetických agentúr disponujúcich takmer neobmedzenými kapacitami. Tento rozdiel robí wiper malvér oveľa nebezpečnejším, pretože namiesto motivácie zisku často sleduje politické, vojenské alebo sabotážne ciele. Zatiaľ čo ransomvérové útoky môžu byť pre firmy obrovským finančným problémom, wiper útoky predstavujú existenčnú hrozbu, ktorá môže ochromiť celé organizácie, vládne inštitúcie alebo kritickú infraštruktúru (NCCIC, 2017).

NotPetya má architektúru kombinujúcu starší proces z roku 2011 známy ako „Mimikatz“, ktorý dovoľoval útočníkom získavať heslá používateľov systému z operačnej pamäte zariadenia a penetračný nástroj „EternalBlue“ umožňujúci využiť slabé miesto v protokoloch Windows pre spustenie škodlivého kódu na každom nezaplátanom systéme. Spojením týchto dvoch prístupov mali hackeri možnosť ukradnúť heslá z nezabezpečeného systému a následne vniknúť do ďalších už aj zaplátaných systémov (Greenberg., 2018).

Na Ukrajine spôsobil NotPetya škody v celonárodnom meradle. Zasiahnutých bolo viacero nemocníc, šesť energetických spoločností, dve letiská, viac než 22 bánk a prakticky každá verejná inštitúcia.

Jedinou ochranou pred malvérom bolo v tom čase odpojenie všetkých počítačov zo siete. Spomedzi prvých zareagovalo ukrajinské ministerstvo zdravotníctva, ktoré odpojilo všetky linky slúžiace na internetové pripojenie. Následkom toho bolo síce zachovanie integrity dát, na druhej strane paralýza viacerých procesov od mzdového účtovníctva po databázu darcov a prijímateľov orgánov (Greenberg, 2019, s. 185-186).

Ešte väčšmi sa následky prejavili na IT systémoch ukrajinskej pošty, ktoré okrem klasických služieb akou je posielanie listov, zabezpečujú prevody peňazí, penzijné platby pre viac než 4,5 milióna dôchodcov ako aj dispečing tisícok poštových áut (Ibid.).

Okrem Ukrajiny sa následky malvéru prejavili paralýzou viacerých firiem a v sumáre miliardovými škodami. Farmaceutická spoločnosť Merck odhadla svoje finančné straty na 1,4 miliardy dolárov, pričom následne podala poistné nároky, ktoré poisťovatelia odmietli uhradiť s odvolaním sa na výnimky týkajúce sa vojnových aktov.

Po dlhoročnom súdnom spore však odvolací súd v New Jersey rozhodol v prospech Mercku, čím potvrdil, že výnimky z poistenia vojny sa na tento prípad nevzťahujú. Tesne pred pojednávaním na Najvyššom súde v New Jersey v roku 2024 spoločnosť dosiahla mimosúdne vyrovnanie s poisťovateľmi (Jones, 2024).

Podobne bola zasiahnutá aj logistická spoločnosť Maersk, ktorá odhadla svoje finančné straty na 300 miliónov dolárov (Wienberg, 2017), logistická spoločnosť TNT Express, ktorá je dcérskou spoločnosťou FedEx zasa 400 miliónov dolárov (FedEx, 2019). Celkový dopad

NotPetya bol vyčíslený na 10 miliárd dolárov, čím sa radí medzi najničivejšie kybernetické útoky v histórii (Geller, 2020).

3 NÁSTROJE V BOJI PROTI KYBERNETICKÝM HROZBÁM

V súčasnosti sa kybernetická bezpečnosť stáva nevyhnutnou súčasťou ochrany kritických infraštruktúr a ekonomických systémov. S rastúcim počtom sofistikovaných kybernetických útokov sa vlády a organizácie po celom svete snažia zaviesť účinné opatrenia na zvýšenie odolnosti voči hrozbám. Jedným z hlavných nástrojov v tejto oblasti sú pokročilé bezpečnostné technológie využívajúce umelú inteligenciu, ktoré umožňujú presnejšie predikovať a detegovať potenciálne útoky, a zároveň legislatívne rámce zaisťujúce efektívnu koordináciu kybernetickej obrany na medzinárodnej úrovni.

V oblasti technologických inovácií predstavujú významný posun riešenia ako Cloud Next-Generation Firewall (NGFW) pre Azure od spoločností Palo Alto Networks a Microsoft, ktorý využíva AI a strojové učenie na detekciu a prevenciu zero-day hrozieb. Tento systém dokáže blokovať takmer 5 miliárd bezpečnostných udalostí denne, čím zvyšuje robustnosť ochrany pred kybernetickými útokmi. Okrem toho pokročilé funkcie, ako je Advanced Threat Prevention, využívajú AI na prediktívne blokovanie útokov typu Command-and-Control (C2), pričom dosahujú viac ako 97 % úspešnosť pri eliminácii týchto hrozieb (Palo Alto Networks, 2023).

Spoločnosť Microsoft na svojom podujatí Microsoft Ignite 2024 predstavila ďalšie inovatívne riešenia, ako je Microsoft Security Copilot, ktorý využíva generatívnu umelú inteligenciu na podporu bezpečnostných a IT tímov pri každodenných operáciách. Tento nástroj umožňuje rýchlejšie identifikovať hrozby, reagovať na ne a znižovať čas na riešenie incidentov až o 30 %. Nový systém Microsoft Security Exposure Management poskytuje organizáciám riešenie na nepretržitú analýzu rizík a ich efektívne zmierňovanie, čím posilňuje celkovú kybernetickú odolnosť (Microsoft, 2024).

Avšak samotné technologické inovácie nie sú postačujúce na komplexné zvládnutie rastúcich kybernetických hrozieb. Z tohto dôvodu sa na regulačnej úrovni zavádzajú právne rámce, ktoré umožňujú efektívnejšiu koordináciu a prevenciu kybernetických útokov. V roku 2024 bol v Európskej únii zavedený Cyber Solidarity Act, ktorý predstavuje mechanizmus solidarity medzi členskými štátmi pri riešení kybernetických incidentov. Dôležitým prvkom tejto iniciatívy je Európsky systém kybernetických varovaní, ktorý združuje národné a cezhraničné Cyber Hubs na rýchlu výmenu informácií o hrozbách a ich efektívnu detekciu v reálnom čase. Okrem toho Kybernetická rezerva EÚ združuje dôveryhodných poskytovateľov bezpečnostných služieb pripravených zasiahnuť v prípade rozsiahlych kybernetických útokov, pričom členské štáty môžu čerpať aj technickú a finančnú podporu na riešenie krízových situácií (Európska komisia, 2024).

Podobný prístup je viditeľný aj v Spojených štátoch, kde bol prijatý Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), ktorý zavádza povinnosť nahlasovať kybernetické incidenty do 72 hodín a ransomvér útoky do 24 hodín agentúre CISA. Tento systém umožňuje rýchlejšie zdieľanie informácií medzi súkromným a verejným sektorom, čím sa posilňuje celková obranyschopnosť krajiny. Navyše, v rámci posilnenia boja proti ransomvérovým útokom bola vytvorená Joint Ransomware Task Force, ktorej úlohou je identifikácia a neutralizácia ransomvérových skupín. Ďalším opatrením je Ransomware Vulnerability Warning Pilot, ktorý umožňuje CISA identifikovať zraniteľné systémy a upozorniť ich prevádzkovateľov na možné riziká (Public Law 117-103, 2022).

Tieto opatrenia, či už na úrovni technologických inovácií alebo regulačných rámcov v EÚ a USA, ukazujú, že boj proti kybernetickým hrozbám je dnes neoddeliteľnou súčasťou globálnej bezpečnostnej stratégie. Kombinácia moderných technológií, regulácií a medzinárodnej spolupráce vedie k budovaniu efektívneho obranného ekosystému, ktorý nielenže reaguje na aktuálne hrozby, ale zároveň umožňuje ich predchádzanie a minimalizáciu potenciálnych škôd.

ZÁVER

Sociálne systémy predstavujú komplexnú sieť vzájomne prepojených štruktúr, ktorých dynamika determinuje stabilitu a funkčnosť spoločnosti. Ich zložitosť spočíva v interakciách medzi jednotlivými aktérmi, regulatívnymi mechanizmami a technologickou infraštruktúrou, čím vzniká adaptívny, no zároveň zraniteľný ekosystém. Každá sociálna skupina totiž nielenže plní špecifické úlohy, ale zároveň moduluje charakter širších spoločenských procesov a ich dlhodobú udržateľnosť.

V kontexte sociotechnických systémov sa ukazuje, že kybernetickú bezpečnosť nemožno redukovať len na technické aspekty. Hoci digitálne bezpečnostné mechanizmy predstavujú dôležitý prvok ochrany, rovnako kľúčové sú aj behaviorálne a organizačné faktory, ktoré ovplyvňujú efektivitu implementovaných stratégií. Práca demonštrovala, že sociálne inžinierstvo predstavuje paradigmatickú výzvu v oblasti kybernetickej bezpečnosti, pretože útočníci čoraz sofistikovanejšie využívajú psychologické a sociálne faktory na obchádzanie tradičných bezpečnostných opatrení.

Potvrdzuje sa, že kybernetické hrozby presahujú individuálnu rovinu a predstavujú kritický faktor v geopolitických, bezpečnostných a ekonomických interakciách. Spektrum kybernetických útokov, od phishingových kampaní po štátom podporované kybernetické operácie, poukazuje na nutnosť multidisciplinárneho prístupu, ktorý spája bezpečnostné, technologické, právne, etické a strategické dimenzie kybernetickej bezpečnosti.

Efektívne a účinné riešenia musia nevyhnutne zahŕňať integráciu technologických inovácií s regulárnymi bezpečnostnými, legislatívnymi a ďalšími opatreniami a vzdelávacími iniciatívami. Optimálny model kybernetickej odolnosti by mal zahŕňať kontinuálne

vzdelávanie, bezpečnostnú a legislatívnu adaptabilitu a čo najširšiu kooperáciu jednotlivých aktérov. Takýto model by zabezpečil nielen prevenciu, ale aj mitigáciu následkov kybernetických incidentov.

Záverom možno konštatovať, že vzájomná previazanosť sociálnych systémov a kybernetickej bezpečnosti vyžaduje holistický a systémový prístup. Udržanie stability digitálne prepojených spoločností predpokladá synergické prepojenie technologickej infraštruktúry, sociálno-organizačných stratégií a bezpečnostných a legislatívnych rámcov. Len tak možno efektívne a účinne čeliť eskalujúcim kybernetickým hrozbám a zabezpečiť dlhodobú ochranu spoločnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BADA, M. - SASSE, A. - NURSE, J. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In International Conference on Cyber Security for Sustainable Society - Conference Proceedings, 2015, s. 118-131.. [online]. [cit. 17.02.2025]. ISSN 2052-8604. Dostupné na internete: <https://lnk.sk/stn0>

BOBOKULOV, A. 2023. The Impact of Social Engineering on Cybercrime: Psychological Manipulation and Prevention Methods. In: International Journal of Cyber Law [online]. Vol. 1, Issue 5, 2023 [cit. 19.01.2025]. Dostupné na internete: <https://lnk.sk/tufj>

DINSTEIN, Y., DAHL, A. W. 2020. Oslo Manual on Select Topics of the Law of Armed Conflict. New York: Springer International Publishing. ISBN978-3-030-39169-0 https://doi.org/10.1007/978-3-030-39169-0

DOUBLEDAY, J. 2024. Biden budget request includes $13B for cybersecurity, continuing upward trend [online]. In: Federal News Network. [cit. 02.02.2025]. Dostupné na internete: <https://lnk.sk/kclt>

DUNN, C. M. - ERIKSEN, C. - SCHARTE, B. 2023. Making cyber security more resilient: adding social considerations to technological fixes. In: Journal of Risk Research [online]. Vol. 26, No. 7, 2023, s. 801-814 [cit. 19.01.2025]. Dostupné na internete: <https://lnk.sk/ebe5> https://doi.org/10.1080/13669877.2023.2208146

EÚ. 2019. Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019, o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty. In EUR-Lex, 2019. [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/btb2>.

EÚ. 2020. Rozhodnutie Rady (SZBP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty. In EUR-Lex, 2020. [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/bszb>.

EÚ. 2024. Korigendum k vykonávaciemu rozhodnutiu Rady (SZBP) 2024/1779 z 24. júna 2024, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L, 2024/1779, 24.6.2024). In EUR-Lex, 2024. [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/fub1>.

EURÓPSKA KOMISIA. 2024. Cyber Solidarity Act [online]. Brussels: European Commission, 2024 [cit. 02.02.2025]. DOSTUPNÉ NA INTERNETE: < https://lnk.sk/ktp9>

FEDERAL TRADE COMMISSION. 2020. Protecting Older Consumers 2019-2020: Report to Congress [online]. Washington, D.C.: FTC, 2020 [cit. 02.02.2025]. Dostupné na internete: <https://lnk.sk/grk3>

FEDEX, 2019. Výročná správa. [online]. p. 53. [cit. 12.01.2025]. Dostupné na internete: <https://lnk.sk/fuho>

GELLER, E., 2020. U.S. charges Russian hackers with sweeping campaign of cyberattacks. [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/rey5>

GREENBERG, A., 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/lgqu>

GREENEBRG, A. 2019. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday s. 185-186.

GYŐFFY, K. - LEITOLD, F. - ARROTT, A. 2017. Individual Awareness of Cyber-Security Vulnerability - Citizen and Public Servant. In: CEE e|Dem and e|Gov Days 2017. Viedeň: Edition Donau-Universität Krems, 2017. s. 411-418. https://doi.org/10.24989/ocg.v325.34

CHOI, Y. B. - RUBIN, J. 2023. Social Engineering Cyber Threats. In: Journal of Global Awareness, [online]. Vol. 4, No. 2, 2023 [cit. 02.02.2025]. Article 8. Dostupné na internete: <https://lnk.sk/lnf0>

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), 2016. Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Cambridge: Cambridge University Press. s. 997-998. https://doi.org/10.1017/9781316755709

IVANČÍK, R. 2012. Kybernetická bezpečnosť - neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012, s. 173-182. ISBN 978-80-8040-450-5.

IVANČÍK, R. 2021. Útočné kybernetické operácie ako súčasť hybridných hrozieb. In Trilobit, 2021, roč. 13, č. 3, 14 s. ISSN 1804-1795.

IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 35-46. ISBN 978-80-8054-998-5.

JANOUŠEK, M., Kyberterorismus: terorismus informační společnosti. In: Defence Strategy [online]. s. 60. [cit. 12.1.2025]. Dostupné na internete: <https://lnk.sk/kwjy>

JIROVSKÝ, V. 2007. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada.

JONES, D., 2024. Merck reaches settlement in closely watched NotPetya insurance case [online]. [cit. 12.01.2025]. DOSTUPNÉ NA INTERNETE: < https://lnk.sk/aknb>

JURČÁK, V. - ANDRASSY, V. - STOLÁRIKOVÁ, K. 2023. Kybernetické operácie ako súčasť kybernetických hrozieb. In Národná a medzinárodná bezpečnosť 2023 : zborník príspevkov z medzinárodnej vedeckej konferencie. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2023, s. 142-150. ISBN 978-80-8040-651-6. https://doi.org/10.52651/nmb.c.2023.9788080406516.142-150

KASPERSKY, 2017. New Petya / NotPetya / ExPetr ransomware outbreak [online]. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/ixpr>

LOURENÇO, A. 2010. Autopoetic Social Systems Theory: The Co-Evolution of Law and the Economy. Cambridge: Centre for Business Research, University of Cambridge, Working Paper No. 409. Dostupné na internete: <https://lnk.sk/bbd1>

LUHMANN, N. 1995. Social Systems. Prel. John Bednarz Jr., Dirk Baecker. Stanford: Stanford University Press, 1995. Pôvodne publikované v nemčine ako Soziale Systeme: Grundriß einer allgemeinen Theorie (1984)

MARTINSKÁ, M. 2019. Výkladový slovník základných sociologických pojmov. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2019. 134 s. ISBN 978-80-8040-586-1.

MATIS, J. - MACIEJEWSKI, J. 2017. Sociologická analýza disponibilných skupín. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, 2017. ISBN 978-80-8040-559-5.

MBA, G. - ONAOLAPO, J. - STRINGHINI, G. - CAVALLARO, L. 2017. Flipping 419 Cybercrime Scams: Targeting the Weak and the Vulnerable. In: WWW '17 Companion. Perth: International World Wide Web Conference Committee (IW3C2), 2017.. ISBN 978-1-4503-4914-7/17/04. Dostupné na internete: <https://lnk.sk/earz>

MEDZINÁRODNÝ SÚDNY DVOR. 1996. Legality of the threat or use of nuclear weapons: Advisory opinion of 8 July 1996 [online]. Haag : International Court of Justice, 1996 [cit. 02.02.2025]. Dostupné na internete: <https://lnk.sk/jycp>

National Cybersecurity and Communications Integration Center (NCCIC), 2017. Destructive Malware [online]. Washington, D.C.: Office of Cybersecurity and Communications, [cit. 02.03.2024]. Dostupné na internete: <https://lnk.sk/lpvi>

PAQUET-CLOUSTON, M. et al., 2019. Ransomware payments in the Bitcoin ecosystem. In: Journal of Cybersecurity [online]. Vol. 5, no. 1, p. 7. [cit. 01.02.2025]. Dostupné na internete: <https://lnk.sk/sypu> https://doi.org/10.1093/cybsec/tyz003

SCHMITT, M. N. et al. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber operations. Cambridge: Cambridge University Press. s. 565. https://doi.org/10.1017/9781316822524.

SPOJENÉ ŠTÁTY AMERICKÉ. Public Law 117-103. Statute at Large 136 Stat. 49 - Public Law No. 117-103 [online]. Washington, D.C.: U.S. Government Publishing Office, 2022 [cit. 02.02.2025]. Dostupné na internete: <https://lnk.sk/aoay>

ŠUBRT, J.: Talcott Parsons a jeho přínos soudobé sociologické teorii. Praha: Karolinum, 2006. 246 s. ISBN 80-146-1239-9

TIKK, E. - KASKA, K. - VIHUL, L. 2010. International Cyber Incidents: Legal Considerations. Tallin: CCD COE. ISBN: 978-9949-9040-0-6

Tlačová správa spoločnosti Microsoft, [cit. 12.1.2025]. Dostupné na internete: <https://lnk.sk/jxgm>

Tlačová správa spoločnosti Palo Alto Networks, [cit. 12.1.2025]. Dostupné na internete: <https://lnk.sk/oeg7>

U.S. SENATE. 2016. Senior Scams: What Are They and How Can People Avoid Them. S. Hrg. 114-848. Hearing before the Special Committee on Aging, 114th Congress, Second Session, March 21, 2016. Washington, D.C.: U.S. Government Publishing Office, 2022. 48 s. Dostupné na internete: <https://lnk.sk/knj7>

WIENBERG, CH. 2017. Maersk Says June Cyberattack Will Cost It up to $300 Million [online]. [cit. 12.01.2025]. Dostupné na internete: <https://lnk.sk/seu5>

JUDr. PhDr. Roman Bartolomej BOROVSKÝ
Akadémia ozbrojených síl M. R. Štefánika
gen. M. R. Štefánika
Demänovská cesta 393, Demänová, 031 01 Liptovský Mikuláš
Tel: +421 903 167 382
e-mail: roman.borovsky@aos.sk