DOI: https://doi.org/10.52651/vr.a.2026.1.68-82
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2026, Číslo 1, Strana 68-82

KYBERNETICKÉ HROZBY V GLOBÁLNEJ POLITIKE: ANALÝZA BEZPEČNOSTNÝCH TRENDOV VO VEDECKOM VÝSKUME

CYBER THREATS IN GLOBAL POLITICS: ANALYSIS OF SECURITY TRENDS IN SCIENTIFIC RESEARCH

Gabriel EŠTOK, Katarína MIŇOVÁ, Michal SILBERG, Jana ANTALÍKOVÁ

História článku

Doručený: 12.01.2026
Schválený: 20.05.2026
Vydaný: 30.06.2026

ABSTRACT

The article focuses on cyber threats in the context of contemporary global politics and the evolving security environment. Its aim is to identify dominant research trends in cybersecurity and analyse their implications for international security and geopolitical relations. The study is based on a systematic review of scientific literature indexed in the Web of Science database between 2013 and 2025. Using qualitative content analysis, more than 160 scholarly publications dealing with cyberattacks, critical infrastructure protection, cyber warfare, hybrid threats, disinformation campaigns and political aspects of cybersecurity were analysed. The findings indicate that cyber threats have evolved from a primarily technical issue into a significant geopolitical and strategic challenge. Since 2022, research has increasingly focused on critical infrastructure protection, cyber resilience, artificial intelligence, hybrid conflicts and the security implications of the war in Ukraine. The analysis also highlights the growing importance of international cooperation, regulatory frameworks and coordinated defence mechanisms in the digital space.

KEYWORDS

cybersecurity, global politics, cyber threats, hybrid threats, geopolitics, critical infrastructure, Web of Science

© 2026 by Author(s). This is an open access article under the Creative Commons Attribution International License (CC BY). http://creativecommons.org/licenses/by/4.0

ÚVOD

Súčasné bezpečnostné prostredie je charakteristické rastúcou mierou geopolitickej nestability, technologickej transformácie a vznikom nových foriem hybridných hrozieb. Digitalizácia spoločnosti, rozvoj informačných technológií a globálna prepojenosť štátov zásadne transformovali charakter bezpečnostných rizík a rozšírili priestor pre vznik netradičných foriem konfliktov. Kybernetický priestor sa postupne stal strategickou doménou,

v ktorej sa prelínajú bezpečnostné, politické, ekonomické a vojenské záujmy štátov i neštátnych aktérov.

Kybernetické hrozby už nemožno vnímať výlučne ako technický problém súvisiaci s ochranou informačných systémov. Ich dôsledky zasahujú fungovanie štátu, kritickej infraštruktúry, ekonomiky, demokratických procesov i medzinárodných vzťahov. Dynamický rozvoj digitálnych technológií, umelej inteligencie, internetu vecí (IoT) a cloudových riešení zároveň vytvára nové zraniteľnosti, ktoré môžu byť zneužité na politické, ekonomické alebo vojenské účely. (Tsakanyan, 2017; Homaniuk, 2024)

Ochrana osobných údajov a bezpečnosť informačných technológií sa čoraz viac stávajú otázkami verejného záujmu, a to najmä v dôsledku rastúcej digitalizácie spoločnosti a exponenciálneho nárastu objemu spracovávaných údajov. Digitalizácia prináša celý rad výhod v oblasti efektivity, komunikácie a riadenia procesov, zároveň však vytvára nové bezpečnostné zraniteľnosti. Rozmach cloudových riešení, internetu vecí, automatizovaných systémov a generatívnej umelej inteligencie zvyšuje riziko zneužitia dát, útokov na dodávateľské reťazce, ransomvérových operácií či sofistikovaných dezinformačných kampaní.

Význam kybernetickej bezpečnosti výrazne vzrástol najmä po roku 2022 v súvislosti s vojnou na Ukrajine, nárastom hybridných operácií, útokov na kritickú infraštruktúru a intenzívnym využívaním informačných operácií v geopolitických konfliktoch. Súčasný bezpečnostný diskurz reflektuje aj rastúce riziká spojené s generatívnou umelou inteligenciou, deepfake technológiami a automatizovanými kybernetickými útokmi. Kybernetický priestor sa tak stal významným nástrojom geopolitického súperenia a strategického presadzovania národných záujmov. (Kostyuk, Zhukov, 2024; Adeyeri, Abroshan, 2024)

Cieľom príspevku je identifikovať dominantné trendy vo vedeckom diskurze týkajúcom sa kybernetických hrozieb a s použitím kvalitatívnych metód výskumu analyzovať ich význam pre globálnu bezpečnosť a medzinárodné vzťahy. Článok vychádza zo systematického prehľadu vedeckej literatúry indexovanej v databáze Web of Science v období rokov 2013–2025 a prostredníctvom obsahovej analýzy a syntézy skúma hlavné tematické línie výskumu kybernetickej bezpečnosti v kontexte globálnej politiky.

V prvej časti článku sú vymedzené základné teoretické koncepty bezpečnosti, bezpečnostných hrozieb a kybernetickej bezpečnosti. Následne sa príspevok zameriava na analýzu digitálnych hrozieb, geopolitických aspektov kybernetických konfliktov a nových trendov vo výskume kybernetickej bezpečnosti po roku 2022. Osobitná pozornosť je venovaná otázkam ochrany kritickej infraštruktúry, hybridným hrozbám, informačným operáciám a rastúcemu významu umelej inteligencie v oblasti kybernetickej bezpečnosti.

1 TEORETICKÉ VYMEDZENIE PROBLEMATIKY

Bezpečnostné prostredie 21. storočia je charakteristické vysokou mierou komplexnosti, dynamiky a vzájomnej prepojenosti jednotlivých rizík a hrozieb. Popri tradičných vojenských hrozbách získavajú čoraz väčší význam netradičné bezpečnostné výzvy, medzi ktoré patria hybridné konflikty, informačné operácie, kybernetické útoky či dezinformačné kampane. Globalizácia, technologický rozvoj a rastúca digitalizácia spoločnosti zároveň významne rozšírili priestor pre vznik nových foriem konfliktov a bezpečnostných zraniteľností. (Masys, 2021; Vilks et al., 2024)

Bezpečnostnú hrozbu možno charakterizovať ako faktor, jav alebo situáciu schopnú narušiť stabilitu, bezpečnosť alebo fungovanie jednotlivca, organizácie alebo štátu. Hrozby môžu mať fyzický, ekonomický, politický, environmentálny alebo digitálny charakter a ich intenzita závisí od miery zraniteľnosti konkrétneho subjektu. Zeman (2002) chápe bezpečnosť ako stav, v ktorom sú vnútorné a vonkajšie hrozby eliminované na čo najnižšiu možnú úroveň a subjekt disponuje schopnosťou efektívne reagovať na existujúce aj potenciálne riziká.

V kontexte súčasného bezpečnostného prostredia sa čoraz väčšia pozornosť venuje pojmu kybernetická bezpečnosť. Kybernetický priestor predstavuje globálnu digitálnu doménu umožňujúcu vytváranie, spracovanie a výmenu informácií prostredníctvom informačných a komunikačných technológií. Zahŕňa technologickú infraštruktúru, počítačové siete, cloudové služby, digitálne platformy, informačné systémy i online komunikačné prostredie.

Kybernetická bezpečnosť predstavuje súbor technických, organizačných, právnych a strategických opatrení zameraných na ochranu informačných systémov, sietí, dát a digitálnej infraštruktúry pred neoprávneným prístupom, zneužitím alebo narušením. Význam kybernetickej bezpečnosti rastie v dôsledku zvyšujúcej sa závislosti spoločnosti od digitálnych technológií a rozširovania kybernetických hrozieb do oblasti geopolitiky, hospodárstva a národnej bezpečnosti. (Pigola, Rezende da Costa, 2023)

Súčasný vývoj zároveň poukazuje na transformáciu kybernetických hrozieb z izolovaných technických incidentov na komplexné strategické nástroje využívané štátmi aj neštátnymi aktérmi. Kybernetické operácie sa stávajú súčasťou hybridných konfliktov, informačných vojen a geopolitického súperenia. Moderné bezpečnostné prostredie preto vyžaduje interdisciplinárny prístup, ktorý reflektuje technologické, politické, ekonomické, právne a psychologické dimenzie kybernetickej bezpečnosti. (Fabio, Berg 2023; Armencheva et al. 2019).

2 METODOLÓGIA

Cieľom nášho výskumu bolo identifikovať dominantné trendy vo vedeckom diskurze týkajúcom sa kybernetických hrozieb a ich významu pre globálnu bezpečnosť a medzinárodné vzťahy. Výskum bol realizovaný formou kvalitatívneho prehľadu vedeckej literatúry

a kvalitatívnej obsahovej analýzy odborných publikácií indexovaných v databáze Web of Science (WoS), ďalej aplikáciou výskumných metód komparácie zdrojov, indukcie, dedukcie a predikcie zistených výsledkov výskumu.

Databáza Web of Science bola zvolená z dôvodu jej vysokej akademickej relevancie, interdisciplinárneho charakteru a zastúpenia recenzovaných vedeckých publikácií z oblasti bezpečnostných štúdií, medzinárodných vzťahov, politológie a kybernetickej bezpečnosti. Výskumný súbor bol vytvorený na základe vyhľadávacieho reťazca využívajúceho Boolean operátory: (Global Politics OR International Relations OR Cyber Threats) AND (Security Risks OR Cybersecurity OR 21st Century Threats) AND (Cybersecurity Policy OR Government Policy OR International Cybersecurity) AND (National Security OR Cyber Warfare OR Defense Strategies).

Vyhľadávanie bolo realizované v období rokov 2013–2025 s dôrazom na publikácie analyzujúce kybernetickú bezpečnosť, kybernetické konflikty, hybridné hrozby, ochranu kritickej infraštruktúry, dezinformačné kampane a geopolitické aspekty digitálnej bezpečnosti. Do výskumného súboru boli zahrnuté výlučne recenzované vedecké články publikované v anglickom jazyku. Vylúčené boli nerelevantné publikácie, duplicitné záznamy, konferenčné abstrakty a práce bez priamej väzby na problematiku bezpečnostných rizík a kybernetických hrozieb.

Zo získaných vedeckých a odborných publikácií boli následne prostredníctvom kvalitatívnej obsahovej analýzy identifikované dominantné tematické kategórie. Analýza bola realizovaná metódou tematického kódovania, pričom jednotlivé štúdie boli klasifikované podľa ich obsahového zamerania. Na základe analytického procesu boli identifikované najmä tieto tematické okruhy:

- kybernetické útoky a ich bezpečnostné dôsledky,
- ochrana kritickej infraštruktúry,
- kybernetické vojny a geopolitické konflikty,
- hybridné hrozby a dezinformačné kampane,
- právne a regulačné aspekty kybernetickej bezpečnosti,
- kybernetická odolnosť a medzinárodná spolupráca.

Osobitná pozornosť bola venovaná vývojovým trendom po roku 2022, ktoré významne ovplyvnili bezpečnostný diškurz v oblasti kybernetickej bezpečnosti, predovšetkým vojenskému konfliktu na Ukrajine, rozvoju generatívnej umelej inteligencie, nárastu ransomvérových útokov a rastúcemu významu ochrany kritickej infraštruktúry.

Limitom nášho výskumu bolo zameranie sa výlučne na databázu Web of Science a anglicky písané publikácie, čo môže obmedzovať zachytenie regionálne špecifických výskumných perspektív. Súčasne ide o dynamicky sa vyvíjajúcu oblasť, v ktorej dochádza k rýchlej transformácii bezpečnostných hrozieb a technologických trendov.

3 DIGITÁLNE HROZBY A TRANSFORMÁCIA BEZPEČNOSTNÉHO PROSTREDIA

Digitalizácia spoločnosti a rastúca závislosť štátov od informačných a komunikačných technológií zásadne transformovali charakter bezpečnostných hrozieb v 21. storočí. Kybernetický priestor sa stal významnou strategickou doménou, v ktorej dochádza k presadzovaniu politických, ekonomických a vojenských záujmov. Moderné kybernetické hrozby už nepredstavujú izolované technické incidenty, ale komplexné bezpečnostné fenomény s potenciálom destabilizovať fungovanie štátu, ekonomiky a spoločnosti.

Podľa odhadov spoločnosti Cybersecurity Ventures môžu globálne ekonomické škody spôsobené kyberkriminalitou do roku 2025 presiahnuť 10 biliónov USD ročne, čo poukazuje na rastúci ekonomický a strategický význam kybernetickej bezpečnosti v globálnom prostredí. (Morgan, 2024)

Odhady Medzinárodnej telekomunikačnej únie (ITU) naznačujú, že v roku 2024 využívalo internet viac ako 5,5 miliardy ľudí na celom svete. Rastúca globalizácia digitálneho priestoru zároveň zvyšuje význam kybernetickej bezpečnosti a rozširuje potenciálne zraniteľnosti moderných spoločností. (ITU, 2024)

Rastúca sofistikovanosť kybernetických útokov súvisí s rozvojom umelej inteligencie, automatizácie a digitálnych technológií. Významný posun možno pozorovať najmä v oblasti ransomware-as-a-service, AI-enabled phishingu, deepfake technológií a automatizovaných dezinformačných kampaní. Generatívna umelá inteligencia zároveň vytvára nové možnosti manipulácie informačného priestoru a zvyšuje efektivitu psychologických a hybridných operácií. (Chen et al., 2024; Backaman, Stevens, 2024)

Správy agentúry ENISA naznačujú, že ransomware patril v období rokov 2022–2024 medzi dominantné kybernetické hrozby zamerané na kritickú infraštruktúru. Podľa ENISA bolo približne 46 % analyzovaných kybernetických incidentov finančne motivovaných, pričom ransomware predstavoval jednu z najčastejších foriem útokov voči strategickým sektorom vrátane energetiky, zdravotníctva a verejnej správy. (ENISA, 2024)

Významným trendom posledných rokov je využívanie generatívnej umelej inteligencie pri realizácii kybernetických operácií. Výskum naznačuje, že AI-enabled cyber attacks výrazne znižujú technickú náročnosť kybernetických útokov a umožňujú automatizáciu phishingových kampaní, tvorbu realistických deepfake materiálov či adaptívnych foriem malvéru. Generatívna AI zároveň zvyšuje efektivitu sociálneho inžinierstva prostredníctvom personalizovaných spear-phishing kampaní a syntetického multimediálneho obsahu, čo komplikuje identifikáciu dôveryhodných informačných zdrojov a zvyšuje riziko informačnej manipulácie. (Chen et. al, 2024)

Kybernetická bezpečnosť sa stala významnou súčasťou národnej aj medzinárodnej bezpečnosti. Rozširovanie digitálnej infraštruktúry a rastúca prepojenosť informačných systémov zvyšujú zraniteľnosť štátov, organizácií i jednotlivcov voči kybernetickým útokom.

Kybernetické incidenty dnes zasahujú široké spektrum oblastí – od verejnej správy, energetiky a dopravy až po zdravotníctvo, finančný sektor či kritickú infraštruktúru. Osobitne významným trendom po roku 2022 sa stali útoky na kritickú infraštruktúru, najmä v oblastiach energetiky, dopravy, zdravotníctva a verejnej správy. Konflikt medzi Ruskom a Ukrajinou poukázal na rastúci význam kybernetických operácií ako súčasti moderných hybridných konfliktov. Kybernetické útoky sa čoraz častejšie využívajú v kombinácii s informačnými operáciami, psychologickým pôsobením a dezinformačnými aktivitami s cieľom oslabiť dôveru verejnosti, destabilizovať spoločnosť a narušiť fungovanie štátnych inštitúcií. (Kostyuk, Zhukov, 2024)

Dnešný svet je výrazne závislý od digitálnych technológií a ochrana dát pred kybernetickými útokmi predstavuje jednu z najväčších bezpečnostných výziev súčasnosti. Integrácia sofistikovaných technológií podporuje inovácie a efektivitu v podnikateľskom i verejnom sektore, zároveň však vytvára nové bezpečnostné riziká. Kybernetické útoky môžu mať ekonomické, politické i vojenské ciele a ich dôsledky môžu zásadne ohroziť stabilitu, rozvoj a bezpečnosť štátu alebo organizácie (Ivančík, Nečas, 2025).

Významným problémom zostáva aj rastúca profesionalizácia kybernetickej kriminality. Kybernetické skupiny dnes fungujú na princípe decentralizovaných medzinárodných sietí a využívajú modely podobné komerčným službám. Zvyšuje sa tiež prepojenie medzi organizovaným zločinom, štátom podporovanými aktérmi a hybridnými bezpečnostnými operáciami.

Ochrana osobných údajov a bezpečnosť informačných systémov sa stávajú otázkami verejného záujmu predovšetkým z dôvodu rastúceho objemu spracovávaných údajov a rozširujúcej sa prítomnosti digitálnych technológií v každodennom živote. Medzi najčastejšie príčiny narušenia bezpečnosti patria ľudská chyba, nesprávna konfigurácia systémov, zastaraný softvér, nedostatočné bezpečnostné opatrenia a phishingové útoky. Významným problémom zostáva aj nedostatok kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti.

S rastúcim počtom kybernetických incidentov sa zvyšuje aj potreba koordinovaných bezpečnostných stratégií a medzinárodnej spolupráce. Výskum naznačuje, že efektívna ochrana digitálneho priestoru si vyžaduje kombináciu technologických riešení, regulačných mechanizmov, strategického riadenia rizík a zvyšovania digitálnej gramotnosti obyvateľstva. (Pigola, Rezende da Costa, 2023)

3.1 Vzostup kybernetických útokov

Rastúca dostupnosť digitálnych technológií a globálna prepojenosť informačných systémov vytvorili priestor pre dynamický rozvoj kybernetickej kriminality a sofistikovaných kybernetických operácií. Kybernetické útoky sú dnes realizované jednotlivcami, organizovanými zločineckými skupinami, hacktivistami aj štátom podporovanými aktérmi. Ich cieľom môže byť získanie citlivých informácií, finančný zisk, destabilizácia štátu alebo presadzovanie geopolitických záujmov.

Významným medzníkom vo vývoji moderných kybernetických hrozieb bol útok NotPetya z roku 2017. Pôvodne lokálny incident prerástol do globálneho kybernetického útoku, ktorý zasiahol nadnárodné korporácie, logistické siete, finančné inštitúcie a kritickú infraštruktúru. Útok demonštroval vysokú mieru zraniteľnosti globálnych dodávateľských reťazcov a zároveň poukázal na prepojenie medzi geopolitickými konfliktmi a kybernetickými operáciami. (Fayi, 2018; Greenberg, 2018)

NotPetya zároveň odhalila riziká spojené s využívaním zraniteľností štátnymi bezpečnostnými agentúrami. Exploit EternalBlue, ktorý bol pri útoku použitý, pochádzal z nástrojov americkej NSA a následne unikol do prostredia kybernetickej kriminality. Incident tak otvoril diskusiu o hraniciach medzi ofenzívnymi kybernetickými kapacitami štátov a globálnou bezpečnosťou digitálneho priestoru. (Dunn Cavelty, Eglof, 2019)

Významným trendom posledných rokov je rastúci počet útokov na dodávateľské reťazce (supply-chain attacks), pri ktorých útočníci kompromitujú softvérových alebo technologických dodávateľov s cieľom zasiahnuť široké spektrum organizácií súčasne. Incidenty ako SolarWinds alebo MOVEit poukázali na vysokú mieru prepojenosti digitálneho prostredia a zraniteľnosť globálnych technologických ekosystémov. Tieto útoky zároveň potvrdzujú, že narušenie jediného článku dodávateľského reťazca môže mať rozsiahle geopolitické, ekonomické a bezpečnostné dôsledky. (Boyens, 2021)

Súčasný vývoj naznačuje posun od izolovaných hackerských útokov smerom ku komplexným hybridným operáciám kombinujúcim kybernetické útoky, informačné operácie, psychologické pôsobenie a dezinformačné kampane. Kybernetické operácie sa tak stávajú integrálnou súčasťou moderných konfliktov a strategického súperenia medzi štátmi.

4 KYBERNETICKÁ BEZPEČNOSŤ AKO GEOPOLITICKÝ NÁSTROJ

Kybernetická bezpečnosť sa v súčasnosti stáva významným nástrojom geopolitického súperenia medzi štátmi. Digitálny priestor umožňuje realizáciu strategických operácií bez potreby priamej vojenskej konfrontácie, čím zásadne mení charakter moderných konfliktov. Štáty aj neštátni aktéri využívajú kybernetické operácie na získavanie spravodajských informácií, destabilizáciu protivníka, ovplyvňovanie verejnej mienky alebo narušenie fungovania kritickej infraštruktúry. (Tsakanyan, 2017; Greiman, 2019)

Kybernetické útoky zároveň predstavujú asymetrický nástroj moci, ktorý umožňuje aj technologicky slabším aktérom zasiahnuť strategické ciele ekonomicky a vojensky silnejších štátov. Významným problémom zostáva atribúcia útokov, keďže identifikácia konkrétneho aktéra býva technicky aj politicky komplikovaná. Táto nejednoznačnosť zvyšuje riziko eskalácie medzinárodného napätia a komplikuje možnosti efektívnej reakcie zo strany medzinárodného spoločenstva. (Rid, 2012; Guchua, Zedelaschvili, 2019)

Významné incidenty posledných rokov, ako útoky na ukrajinskú infraštruktúru, zásahy do volebných procesov či rozsiahle dezinformačné operácie, potvrdzujú rastúci význam

kybernetických operácií v geopolitickom prostredí. Kybernetický priestor sa stal významnou dimenziou hybridných konfliktov, v ktorých sa kombinujú informačné operácie, psychologické pôsobenie, ekonomický tlak a digitálne útoky.

Vojenský konflikt medzi Ruskom a Ukrajinou predstavuje významný míľnik vo vývoji moderných hybridných konfliktov. Konflikt poukázal na intenzívne prepájanie kybernetických operácií, informačných kampaní, psychologického pôsobenia a tradičných vojenských aktivít. Kybernetické útoky na energetickú infraštruktúru, komunikačné siete a štátne informačné systémy zároveň demonštrovali rastúci význam digitálneho priestoru ako integrálnej súčasti moderného bojového prostredia. Výskum po roku 2022 zároveň reflektuje rastúcu úlohu spolupráce medzi štátom a súkromným sektorom pri ochrane kritickej infraštruktúry a zabezpečovaní kybernetickej odolnosti. (Kostyuk, Zhukov, 2024)

Výskumné štúdie zároveň poukazujú na rastúci význam konceptu digitálnej suverenity, v rámci ktorého sa štáty snažia posilňovať kontrolu nad vlastnou digitálnou infraštruktúrou, dátami a technologickými kapacitami. Kybernetická bezpečnosť sa tak postupne transformuje z technickej oblasti na integrálnu súčasť strategického a geopolitického rozhodovania. (Couture, Toots, 2023)

Rastúci význam digitálnej suverenity reflektuje snahu štátov posilňovať kontrolu nad dátovou infraštruktúrou, cloudovými riešeniami, technologickými platformami a strategickými digitálnymi kapacitami. Geopolitická rivalita medzi Spojenými štátmi, Čínou a Európskou úniou zároveň poukazuje na rastúci význam technologickej autonómie, kontroly polovodičového priemyslu a ochrany strategických dátových tokov. Kybernetická bezpečnosť sa tak stáva významnou súčasťou ekonomickej a geopolitickej konkurencieschopnosti štátov. (Couture, Toots, 2023)

4.1 Riziká pre kritickú infraštruktúru

Jednou z najvýznamnejších oblastí súčasných kybernetických hrozieb je ochrana kritickej infraštruktúry. Energetické siete, zdravotnícke systémy, dopravná infraštruktúra, telekomunikačné siete či finančné systémy predstavujú strategické sektory, ktorých narušenie môže mať rozsiahle ekonomické, sociálne a bezpečnostné dôsledky. (Homaniuk, 2024, Yerina et al. 2021)

Kybernetické útoky na kritickú infraštruktúru môžu spôsobiť prerušenie dodávok energií, výpadky zdravotníckych systémov, ochromenie dopravy alebo destabilizáciu finančných trhov. Rastúci význam smart technológií a internetu vecí zároveň rozširuje množstvo potenciálnych zraniteľností. Výskum po roku 2022 reflektuje rastúcu potrebu budovania kybernetickej odolnosti kritických sektorov a koordinácie bezpečnostných opatrení na národnej i medzinárodnej úrovni.

Súčasný bezpečnostný diskurz zároveň reflektuje posun od tradičného modelu prevencie kybernetických incidentov smerom ku konceptu kybernetickej odolnosti (cyber

resilience). Tento prístup zdôrazňuje schopnosť štátu, organizácií a kritickej infraštruktúry absorbovať, adaptovať sa a obnoviť svoje fungovanie po kybernetickom incidente. Výskumné štúdie po roku 2022 čoraz intenzívnejšie poukazujú na potrebu budovania resilientných systémov schopných zabezpečiť kontinuitu fungovania aj v podmienkach hybridných konfliktov a rozsiahlych kybernetických útokov. (Linkov, Kott, 2019).

4.2 Dezinformácie a psychologické operácie

Významnou súčasťou moderných hybridných konfliktov sa stali dezinformačné kampane a psychologické operácie realizované prostredníctvom digitálneho priestoru. Sociálne siete, online platformy a digitálne médiá umožňujú rýchle šírenie manipulatívneho obsahu, polarizáciu spoločnosti a ovplyvňovanie verejnej mienky.

Rozvoj generatívnej umelej inteligencie zároveň výrazne zvyšuje potenciál tvorby realistického manipulatívneho obsahu vrátane deepfake videí, syntetických hlasových záznamov a automatizovaných informačných kampaní. Tieto technológie vytvárajú nové bezpečnostné výzvy nielen pre štáty, ale aj pre demokratické procesy, mediálne prostredie a spoločenskú dôveru. (Chen, 2024)

Moderné hybridné operácie sa čoraz viac orientujú na kognitívnu dimenziu konfliktov, ktorej cieľom je ovplyvňovanie percepcie, dôvery a rozhodovacích procesov spoločnosti. Koncept cognitive warfare zdôrazňuje využívanie digitálnych technológií, sociálnych sietí a informačných operácií na formovanie verejnej mienky a destabilizáciu spoločenského prostredia bez potreby priamej vojenskej konfrontácie. Výskum naznačuje, že kognitívna dimenzia bezpečnosti bude v nasledujúcich rokoch predstavovať jednu z najvýznamnejších výziev pre demokratické štáty. (Claverie, Du Cluzel, 2022)

5 NOVÉ TRENDY KYBERNETICKÝCH HROZIEB PO ROKU 2022

Výskum odborných publikácií indexovaných v databáze Web of Science poukázala na dominantné tematické zameranie výskumu v oblasti kybernetickej bezpečnosti po roku 2020. Najvýraznejšie zastúpené boli štúdie zamerané na kybernetické útoky, hybridné hrozby, ochranu kritickej infraštruktúry a geopolitické aspekty kybernetických konfliktov. Po roku 2022 možno zároveň identifikovať výrazný nárast výskumného záujmu o problematiku umelej inteligencie, kybernetickej odolnosti a bezpečnostných dôsledkov vojny na Ukrajine.

Vývoj bezpečnostného prostredia po roku 2022 významne ovplyvnil charakter vedeckého diskurzu v oblasti kybernetickej bezpečnosti. Analýza odbornej literatúry naznačuje posun výskumného záujmu od tradičných otázok ochrany informačných systémov smerom ku komplexnej problematike kybernetickej odolnosti, hybridných konfliktov a geopolitických dôsledkov digitálnych technológií. (Backman, Stevens, 2024)

Významným faktorom transformácie bezpečnostného diskurzu sa stal vojenský konflikt medzi Ruskom a Ukrajinou, ktorý poukázal na strategický význam kybernetických operácií

v moderných ozbrojených konfliktoch. Kybernetické útoky na energetickú infraštruktúru, komunikačné siete a štátne informačné systémy potvrdili, že digitálny priestor predstavuje integrálnu súčasť súčasných hybridných vojen. Výskum zároveň poukazuje na čoraz intenzívnejšie prepájanie kybernetických operácií s informačnými a psychologickými aktivitami zameranými na destabilizáciu spoločnosti a ovplyvňovanie verejnej mienky. (Kostyuk, Zhukov, 2024)

Výrazný posun možno pozorovať aj v oblasti umelej inteligencie a jej využívania v kybernetických operáciách. Generatívna AI umožňuje tvorbu sofistikovaných phishingových kampaní, automatizovaných dezinformačných operácií a realistického manipulatívneho obsahu. Deepfake technológie a voice cloning predstavujú nové bezpečnostné riziká, ktoré komplikujú identifikáciu dôveryhodných informačných zdrojov a zvyšujú potenciál informačnej manipulácie. (Chen et al., 2024)

Výskumné štúdie publikované po roku 2023 zároveň upozorňujú na rastúci význam AI-enabled cyber attacks, ktoré výrazne znižujú technickú náročnosť realizácie kybernetických útokov. Automatizované nástroje umožňujú rýchlejšiu identifikáciu zraniteľností, adaptívne formy malvéru a efektívnejšie cielenie útokov na jednotlivcov aj organizácie.

Významným trendom súčasného bezpečnostného prostredia je aj rastúca profesionalizácia kybernetickej kriminality. Model ransomware-as-a-service umožňuje decentralizovaným skupinám realizovať rozsiahle útoky bez potreby pokročilých technických znalostí. Kybernetická kriminalita sa tak postupne transformuje na globálny ekonomický ekosystém prepájajúci organizovaný zločin, digitálne technológie a geopolitické záujmy. (Ibrar et al., 2024)

Súčasný vývoj reflektuje aj rastúci význam regulačných a strategických prístupov ku kybernetickej bezpečnosti. Európska únia v reakcii na rastúce bezpečnostné riziká prijala smernicu NIS2, ktorá zdôrazňuje potrebu posilňovania kybernetickej odolnosti kritických sektorov a koordinácie bezpečnostných opatrení na nadnárodnej úrovni. Výskum zároveň reflektuje rastúci význam konceptov cyber resilience, digital sovereignty a collective cyber defence. Prijatie smernice NIS2 zároveň poukazuje na rastúcu institucionalizáciu kybernetickej bezpečnosti na úrovni Európskej únie. Nový regulačný rámec rozširuje požiadavky na ochranu kritických sektorov a zdôrazňuje význam koordinovaného riadenia kybernetických rizík, incident reporting mechanizmov a strategickej pripravenosti členských štátov. Vývoj regulačných opatrení zároveň reflektuje rastúce prepojenie medzi národnou bezpečnosťou, digitálnou infraštruktúrou a geopolitickou stabilitou. (European Union, 2022)

Rastúca internacionalizácia kybernetických hrozieb zároveň potvrdzuje potrebu intenzívnejšej medzinárodnej spolupráce v oblasti zdieľania informácií, koordinácie obranných mechanizmov a tvorby spoločných regulačných rámcov. Súčasné bezpečnostné prostredie naznačuje, že efektívne zvládanie kybernetických hrozieb si vyžaduje multidisciplinárny prístup prepájajúci technologické, bezpečnostné, právne, politické a spoločenské aspekty digitálnej bezpečnosti.

ZÁVER

Kybernetické hrozby predstavujú jednu z najvýznamnejších bezpečnostných výziev súčasného globálneho prostredia. Analýza vedeckej literatúry indexovanej v databáze Web of Science poukazuje na výraznú transformáciu bezpečnostného diskurzu v období rokov 2013–2025, počas ktorého sa kybernetická bezpečnosť postupne etablovala ako významná geopolitická, strategická a spoločenská téma.

Výsledky výskumu naznačujú rastúci dôraz na problematiku ochrany kritickej infraštruktúry, hybridných hrozieb, dezinformačných kampaní a kybernetických operácií realizovaných v kontexte geopolitických konfliktov. Významný posun vo výskumnom diskurze možno identifikovať najmä po roku 2022, keď vojenský konflikt na Ukrajine a rozvoj generatívnej umelej inteligencie výrazne zvýšili pozornosť venovanú otázkam kybernetickej odolnosti, digitálnej suverenity a kolektívnej obrany v kybernetickom priestore. (Kostyuk & Zhukov, 2024, Chen et al. 2024)

Náš výskum zároveň potvrdzuje, že kybernetické hrozby nemožno redukovať výlučne na technický problém ochrany informačných systémov. Ich dôsledky zasahujú fungovanie štátu, medzinárodné vzťahy, ekonomickú stabilitu, demokratické procesy i spoločenskú dôveru. Kybernetická bezpečnosť sa tak stáva integrálnou súčasťou moderného bezpečnostného a geopolitického prostredia.

Môžeme konštatovať, že súčasný vývoj zároveň naznačuje potrebu multidisciplinárneho prístupu ku skúmaniu kybernetických hrozieb, ktorý bude reflektovať technologické, politické, právne, ekonomické a psychologické aspekty digitálnej bezpečnosti. Dynamický charakter kybernetického priestoru zároveň vytvára priestor pre ďalší výskum zameraný na dôsledky umelej inteligencie, hybridných konfliktov a rastúcej internacionalizácie kybernetických operácií. (Vilks et al. 2024, Fabio, Berg, 2023).

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ABBASI, S. N. 2023. U.S.-China Cyber Warfare in the 21st Century: Implications for International Security. *Insight Turkey*, *25*. DOI: https://doi.org/10.25253/99.2023252.10

ALBAHAR, M. A. 2019. Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4), s. 993-1006. DOI: https://doi.org/10.1007/s11948-016-9864-0

ADEYERI, A., & ABROSHAN, H. 2024. Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682. DOI: https://doi.org/10.3390/info15110682

ARADAU, C. 2016. *Risk, (in)security and international politics*. s. 308-316. DOI: https://doi.org/10.4324/9781315776835.CH25 https://doi.org/10.4324/9781315776835-40

ARMENCHEVA, I. et al., 2019. Cyber globalization as an in/stability factor. *IJASOS- International E-Journal of Advances in Social Sciences*, *5*(13), s. 71-81. DOI: https://doi.org/10.18769/ijasos.531497

BACHMANN, S.D.D., & GUNNERIUSSON, H. (2014). Terrorism and cyber attacks as hybrid threats : defining a comprehensive approach for countering 21st century threats to global peace and security. *Social Science Research Network*, *9*(1), s. 26-36. DOI: https://doi.org/10.2139/ssrn.2252595

BEGISHEV, I.R., et al,. 2019. Information Infrastructure of Safe Computer Attack. *HELIX, 9*(5), s. 5639-5642. DOI: https://doi.org/10.29042/2019-5639-5642

BIALOSKÓRSKY, R. 2012. Cyberthreats in the Security Environment of the 21st Century: Attempt of the Conceptual Analysis. *Journal of Security and Sustainability Issues*, *1*(4), s. 249-260. DOI: https://doi.org/10.9770/jssi.2012.1.4(2)

BACKMAN, S., & STEVENS, T. 2024. Cyber risk logics and their implications for cybersecurity. *International Affairs, 100*(6), s. 2441-2460. DOI: https://doi.org/10.1093/ia/iiae236

BOZONELOS, D., & TSAGDIS, D. 2023. From Fragmented Geopolitics to Geopolitical Resilience in International Business. *AIB Insights, 23*(2). DOI: https://doi.org/10.46697/001c.73803

BOYENS, J. et al. 2021. Software Supply Chain Attacks. National Institute of Standards and Technology (NIST). DOI: https://doi.org/10.6028/NIST.CSWP.04262021

CLAVERIE, B., & DU CLUZEL, F. 2022. Cognitive Warfare: The Future of Cognitive Dominance. NATO Innovation Hub. Dostupné z: https://lnk.sk/ou069

COUTURE, S., & TOOTS, M. 2023. Digital Sovereignty in the European Union: Challenges and Strategic Implications. Policy & Internet, 15(4). DOI: https://doi.org/10.1002/poi3.337

CHEN, Q. et al. 2024. Artificial Intelligence and Cybersecurity: Opportunities and Threats in the Digital Era. Computers & Security, 137. DOI: https://doi.org/10.1016/j.cose.2024.103756

DOUGLASS, M. 2000. Globalization and the pacific asia crisis—toward economic resilience through livable cities. *Asian Geographer, 19*, 119–137. DOI: https://doi.org/10.1080/10225706.2000.9684066

DUIC, I. et al. 2017. International cyber security challenges. *International Convention on Information and Communication Technology, Electronics and Microelectronics*, s. 1309-1313. DOI: https://doi.org/10.23919/MIPRO.2017.7973625

EUROPEAN UNION. 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

ENISA. 2024. *ENISA Threat Landscape 2024.* Luxembourg: Publications Office of the European Union. European Union Agency For Cybersecurity. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

FABIO, C. & BERG, B. 2023. *Hybridity, Conflict, and the Global Politics of Cybersecurity*. Rowman & Littlefield, Lanham. DOI: https://doi.org/10.5771/9781538170168

FARWELL, J.P., & ROHOZINSKY, R. 2011. Stuxnet and the Future of Cyber War. *Survival, 53*(1), s. 23-40. DOI: https://doi.org/10.1080/00396338.2011.555586

Fayi, S.Y.A. 2018. What Petya/NotPetya Ransomware Is and What Its Remidiations Are. In: Information Technology—New Generations, Springer International Publishing, 93-100. DOI: https://doi.org/10.1007/978-3-319-77028-4_15

GREENBERG, A. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired, August 22. Dostupné z: https://lnk.sk/twkp8

GREIMAN, V. A. 2019. *The Winds of Change in World Politics and the Impact on Cyber Stability*. *9*(4), 27-43. DOI: https://doi.org/10.4018/IJCWT.2019100102

GUCHUA, A., & ZEDELASHVILI, T. 2019. *Cyberwar as a Phenomenon of Asymmetric Threat and Cyber-Nuclear Security Threats*. *40*, 50–57. DOI: https://doi.org/10.31861/MHPI2019.40.50-57

HOMANIUK, O. 2024. Cybersecurity as a component of the international security. Ad Alta, 14(2), s. 90-93. Dostupné z: https://www.magnanimitas.cz/ADALTA/140244/PDF/140244.pdf

HRYBINENKO, O. 2019. *International economic security: assessment of the modern environment, global trends and risk factors*. *149*, s. 14-22. Dostupné z: https://doi.org/10.32782/2224-6282/149-2

IVANČÍK, R. 2024. Bezpečnostné implikácie globalizácie vo vybraných sférach modernej ľudskej spoločnosti. *Vojenské Reflexie*, *19*(2), s. 32–53. DOI: https://doi.org/10.52651/vr.a.2024.2.32-53

IVANČÍK, R. & NEČAS, P. 2025. *Hybridné hrozby: Bezpečnostná výzva pre demokratické spoločnosti*. Praha : Leges. 226 s. ISBN 978-80-7502-823-5.

IVANČÍK, R. & NEČAS, P. 2025. The role and influence of the conspiratorial narrative on the acceptance of conspiracy theories. *Entrepreneurship and Sustainability Issues, 2024, Vol. 12, no. 4, p. 158-170*. ISSN 2345-0282. DOI: https://doi.org/10.9770/x8354649666

IBRAR, M. et al. 2024. Comprehensive review of emerging cybersecurity trends and developments. *International Journal of Electronic Security and Digital Forensic, 16*(5). DOI: https://doi.org/10.1504/IJESDF.2024.140762

ITU. 2024. INTERNATIONAL TELECOMMUNICATION UNION. *Facts and Figures 2024*. Geneva: ITU. Dostupné z: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/

KHAUSTOVA, V. Y., & TRUSKHINA, N. 2024. Risks and Threats to National Security: Essence and Classification. *Business Inform*, *10*(561), s. 6–22. DOI: https://doi.org/10.32983/2222-4459-2024-10-6-22

LINKOV, I., & KOTT, A. 2019. Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Cyber Resilience of Systems and Networks. Springer. DOI: https://doi.org/10.1007/978-3-319-77492-3_1

MANISZEWSKA, K. 2024. Globalization of Security Threats: A Vicious Circle. *Social Inclusion*, *12*. DOI: https://doi.org/10.17645/si.8717

MARI, W. 2022. *Introduction*, s. 1-14. DOI: https://doi.org/10.4324/9781003110224-1

MASYS, A. J. 2021. *The Security Landscape—Systemic Risks Shaping Non-traditional Security*. s. 1-14. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-71998-2_1

MORGAN, S. 2024. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybersecurity Ventures. Dostupné z: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

KALDOR, M., & RANGELOV, I. 2014. *The handbook of global security policy*. John Wiley & Sons. Dostupné z: http://eprints.lse.ac.uk/57273/. DOI: https://doi.org/10.1002/9781118442975

KIVSHYK, O., & KOTELEVETS, M. 2023. Threats to the economic security of the state under global transformations. *Economic Scope*. DOI: https://doi.org/10.32782/2224-6282/183-4

KOSTYUK, N., & ZHUKOV, Y. 2024. Invisible Digital Front: Cyber Operations in Russia's War Against Ukraine. *Journal of Strategic Studies, 47(2).* DOI: https://doi.org/10.1080/01402390.2023.2263978

McGRAW, G. 2013. Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies, 36*(1), s. 109-119. DOI: https://doi.org/10.1080/01402390.2012.742013

MOAGAR-POLADIAN, S., & DRAGOI, A. E. 2015. Crimean Crisis Impact on International Economy: Risks and Global Threats. *Procedia. Economics and Finance*, *22*, s. 452-462. DOI: https://doi.org/10.1016/S2212-5671(15)00238-5

PAVIĆEVIĆ, M., & KARIM, M. R. 2024. *Great Power Competition and Cyber Security*, s. 89102. DOI: https://doi.org/10.1007/978-981-99-9424-3_6

PIGOLA, A., & REZENDE da COSTA, P. 2023. Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. *Communications of the Association for Information Systems*, *53*(1), s. 1099-1135. DOI: https://doi.org/10.17705/1CAIS.05347

RID. T. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), s. 5-32, DOI: https://doi.org/10.1080/01402390.2011.608939

ROMARINA, A. 2016. Economic Resilience Pada Industri Kreatif Gunamenghadapi Globalisasi Dalam Rangka, *Ketahanan Nasional. 15*(1), 35–52. DOI: https://doi.org/10.14710/JIS.15.1.2016.35-52

STANŃCZYK, J. 2022. Managing complex geopolitical threats in the contemporary world. *Przegląd Nauk o Obronności*, *13*, s. 1-27. DOI: https://doi.org/10.37055/pno/152385

SIMMONDS, K. C., & LOUIME, C. J. 2023. Global Resilience Nexus: Forging a Sustainable Future. *American Journal of Environmental Sciences 19*(4), s. 87-106, DOI: https://doi.org/10.3844/ajessp.2023.87.106

SRIKANTH, D. 2014. *Non-traditional security threats in the 21st century: A review*. *4*(1), s. 60-68. Dostupné z: http://www.ijdc.org.in/uploads/1/7/5/7/17570463/2014junearticle4.pdf

STAVYTSKYY, A. 2018. *Influence Of Modern Geopolitical Challenges On State'S Economic Security*. *199*, s. 45-55. Dostupné z: https://ideas.repec.org/a/scn/pnoeeq/199a6.html

TSAKANYAN, V. T. 2017. *The role of cybersecurity in world politics*. *17*(2), s. 339-348. DOI: https://doi.org/10.22363/2313-0660-2017-17-2-339-348

VNUCHKO, S. et al., 2024. *Information terrorism and its prevention in the global political environment in the 21st century*. DOI: https://doi.org/10.33543/1401396368

VILKS, A., et al. 2024. Challenges in Building a Secure Sustainable Society Amid Global Risks and Threats: Theoretical and Practical Aspects. *European Journal of Sustainable Development*, *13*(3), 125. DOI: https://doi.org/10.14207/ejsd.2024.v13n3p125

VAUGHAN, E. J. 1997. *Risk management*. New York: John Wiley. ISBN 0-471-10759-X.

YERINA, A.M. et al., 2021. Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation. 17*(3), s. 3-13, DOI: https://doi.org/10.15407/scine17.03.003

YATSENKO, O. et al. 2018. *The impact of global risks on the world trade and economic environment*. *4*(27), s. 435-444. DOI: https://doi.org/10.18371/FCAPTP.V4I27.154279

ZAVAZAVA. C. L. 2025. Global Cybersecurity Index 2024. Dostupné z: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

ZEMAN, P. 2002. *Česká bezpečnostní terminologie: výklad základních pojmů*. Sborníky. Brno: Masarykova univerzita, Mezinárodní politologický ústav. ISBN 80-210-3037-2.

Vyhlásenie o dostupnosti údajov: Viac informácií a údajov je možné získať od autorov na základe žiadosti.
Príspevky autorov: Autori prispeli rovnakým dielom, prečítali si a súhlasili s publikovanou verziou rukopisu.

doc. Mgr. Gabriel EŠTOK, PhD.
FVS UPJŠ - Univerzita Pavla Jozefa Šafárika v Košiciach, Fakulta verejnej správy
e-mail: gabriel.estok@upjs.sk
ORCID iD: 0000-0001-7269-1814

Mgr. Katarína MIŇOVÁ, PhD
FVS UPJŠ - Univerzita Pavla Jozefa Šafárika v Košiciach, Fakulta verejnej správy
e-mail: katarina.minova@upjs.sk
ORCID ID: 0000-0002-5135-7427

Ing. Bc. Michal SILBERG, MBA, MSc.
FPVaMV UMB - Univerzita Mateja Bela v Banskej Bystrici, Fakulta politických vied a medzinárodných vzťahov
e-mail: michal.silberg@umb.sk
ORCID ID: 0009-0009-7910-362X

Ing. Jana ANTALÍKOVÁ, MBA
Vysoká škola bezpečnostného manažérstva v Košiciach,
e-mail: jana.antal1004@gmail.com
ORCID iD: 0009-0004-5259-4733