O KYBERNETICKEJ BEZPEČNOSTI A OBRANE EURÓPSKEJ ÚNIE V KONTEXTE KONFLIKTU NA UKRAJINE

ON CYBER SECURITY AND DEFENSE OF THE EUROPEAN UNION IN THE CONTEXT OF THE CONFLICT IN UKRAINE

plk. gšt. v. z. doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu,
Sklabinská 1, 835 17 Bratislava, Slovenská republika
radoslav.ivancik@akademiapz.sk

Abstract: The Russian invasion of Ukraine, despite many indications, caused a shock to European countries and returned the almost forgotten features of power politics to the European continent in the form of an interstate conflict and a war of conquest. An integral part of this conflict are the cyber operations carried out by Russian state and non-state actors on Ukrainian targets, which, among many other things, once again drew attention to the need to increase the level of cyber security and defence of the European Union as a whole and its member states. This is also why the author, following the outbreak of the conflict in Ukraine, using relevant methods of interdisciplinary scientific research, deals in this article with the issue of cyber security and defence at the EU level.

Keywords: European Union, cyber security, cyber defence, cyber war, cyber attacks.

Abstrakt: Ruská invázia na Ukrajinu spôsobila napriek mnohým indíciám európskym krajinám šok a vrátila takmer už zabudnuté črty mocenskej politiky na európsky kontinent v podobe medzištátneho konfliktu a dobyvačnej vojny. Nedeliteľnou súčasťou tohto konfliktu sú kybernetické operácie realizované ruskými štátnymi aj neštátnymi aktérmi na ukrajinské ciele, čo okrem množstva iných vecí opätovne upriamilo pozornosť na nutnosť zvyšovania úrovne kybernetickej bezpečnosti a obrany Európskej únie ako celku a aj jej členských štátov. Aj preto sa autor, v nadväznosti na vypuknutie konfliktu na Ukrajine, s využitím relevantných metód interdisciplinárneho vedeckého výskumu, zaoberá v tomto článku problematikou kybernetickej bezpečnosti a obrany na úrovni EÚ.

Kľúčové slová: Európska únia, kybernetická bezpečnosť, kybernetická obrana, kybernetická vojna, kybernetické útoky.

ÚVOD

Európska únia (ďalej len „EÚ“ alebo „Únia“) vzhľadom na súčasný vývoj (nielen) na európskom kontinente, ktorý je v posledných rokoch poznačený kontinuálnym zhoršovaním globálneho i regionálneho bezpečnostného prostredia, zhoršovaním bezpečnostnej situácie v jej bližšom i vzdialenejšom okolí a zvyšovaním napätia vo vzťahoch medzi štátmi, predovšetkým medzi súperiacimi veľmocami, v ostatných rokoch podnikla niektoré dôležité kroky k zvýšeniu úrovne zaistenia jej bezpečnosti a obrany. Tieto kroky napríklad v podobe Stálej štruktúrovanej spolupráce[1] (Permanent Structured Cooperation – PESCO), Európskeho obranného fondu[2] (European Defence Fund – EDF), Spôsobilostí vojenského plánovania a vedenia (Military Planning and Conduct Capability – MPCC) alebo Strategického kompasu[3] (Strategic Compass – SC) realizovala v rámci rozvoja Spoločnej bezpečnostnej a obrannej politiky (ďalej len „SBOP“) Únie, predovšetkým jej obrannej časti.

Členské štáty EÚ sa zároveň s využitím príležitostí, ktoré poskytuje Lisabonská zmluva po ruskej anexii Krymu v roku 2014 a Brexite v roku 2020, aj vzhľadom na presmerovanie strategických záujmov Spojených štátov amerických (ďalej len „USA“) do Ázie a Tichomoria[4], rozhodli, že budú vyčleňovať zo svojich rozpočtov viac zdrojov na zvýšenie svojich obranných spôsobilostí a kapacít, v rámci toho rozvíjať spoločné projekty a že prijmú nový rámec na posilnenie strategickej autonómie Európy.[5] Toto rozhodnutie nadobudlo po vpáde jednotiek Ozbrojených síl Ruskej federácie na ukrajinské územie novú dimenziu. Ruská invázia na Ukrajinu totiž napriek mnohým indíciám spôsobila európskym štátom šok a vrátila takmer už zabudnuté črty mocenskej politiky na európsky kontinent v podobe medzištátneho konfliktu a dobyvačnej vojny.

EÚ však dokázala napriek silnému exogénnemu šoku veľmi rýchlo reagovať na Rusko, keď prijala celú sériu nových sankcií proti Putinovmu režimu (a tiež proti Lukašenkovmu režimu v Bielorusku)[6] a súčasne využila Európsky mierový nástroj[7] (European Peace Facility – EPF) na podporu dodávok vojenského materiálu a techniky z členských štátov Únie do Kyjeva. EÚ tak po prvýkrát vo svojej histórii využíva špecializovaný mimorozpočtový nástroj na financovanie smrtiaceho vojenského vybavenia pre tretiu krajinu.[8] Okrem toho európske

---

1 EDA. Permanent Structured Cooperation. In *European Defence Agency*, 2022.
2 EDA. European Defence Fund. In *European Defence Agency*, 2022.
3 Európska rada. A Strategic Compass for a stronger EU security and defence in the next decade. In *European Council*, 2022.
4 BLACKWILL, R. D. The U.S. Pivot to Asia and American Grand Strategy. In *Council on Foreign Relations*, 2018.
5 FIOTT, D. Strategic autonomy: towards ‘European sovereignty’ in defence? In *European Union Institute for Security Studies*, 2018.
6 Európska rada. EU sanctions against Russia explained. In *European Council*, 2022..
7 Európska komisia. European Peace Facility. In European Commission – Service for Foreign Policy Instruments, 2022.
8 BILQUIN, B. Russia’s war on Ukraine: The EU’s financing of military assistance to Ukraine. In *European Parliamentary Research Centre*, 2022.

krajiny posielajú vojenskú techniku a materiál na Ukrajinu aj na bilaterálnej báze. Takáto reakcia spolu s rozhodnutím podporiť viaceré balíky sankcií napriek ich negatívnym dopadom na ekonomiky členských štátov EÚ poukazuje na značnú mieru angažovanosti Únie v konflikte na Ukrajine.

Členské štáty EÚ, ako vyplýva z vyššie uvedeného, podnikli v reakcii na ruskú agresiu množstvo politických a vojenských rozhodnutí a opatrení. V tomto kontexte zaujíma osobitné miesto kybernetická doména, čiastočne kvôli jej jedinečnej povahe (ako prostredie vytvorené výlučne človekom, ktoré je väčšinou v súkromnom vlastníctve a prevádzke), a čiastočne aj kvôli úlohe, ktorú zohráva v prebiehajúcom konflikte. Aj preto sa autor, využijúc relevantné metódy interdisciplinárneho vedeckého výskumu (najmä analyticko-syntetickú metódu, obsahovú a kvalitatívnu analýzu, analýzu štúdia dokumentov a pod.), v nadväznosti na vypuknutie konfliktu na Ukrajine zaoberá v tomto článku problematikou kybernetickej bezpečnosti a obrany na úrovni EÚ.

KYBERNETICKÁ VOJNA NA UKRAJINE?

Pred začatím ruskej invázie a dokonca aj v prvých dňoch konfliktu väčšina analytikov a expertov predpokladala, že Rusko sa uchýli k masívnym kybernetickým útokom a rušivým akciám v období pred a počas kinetickej vojenskej operácie. Moskva už pred rokom 2014 aj po ňom (opakovane a často úspešne) použila kybernetické „zbrane“ proti Kyjevu, zamerané na energetickú infraštruktúru, vládne agentúry a komunikačné siete. Všeobecným predpokladom teda bolo, že aj v prípade nejakej formy priamej konfrontácie s Kyjevom využije svoje aktíva a schopnosti v tejto oblasti. Ešte koncom februára sa všetky západné spravodajské služby pri poskytovaní rôznych hodnotení týkajúcich sa vojenskej agresie zo strany Ruska zhodli na pravdepodobnosti nadchádzajúcich nepriateľských kybernetických operácií s destabilizačným, rušivým a podvratným zámerom.[9]

V kyberpriestore ruskí aktéri, medzi ktoré patrí (ne)slávne známa agentúra pre výskum internetu so sídlom v Petrohrade a množstvo takzvaných pokročilých perzistentných hrozieb[10] (Advanced Persistent Threat – APT) ako Fancy Bear, Cozy Bear a Sandworm – majú tendenciu

---

[9] CERULUS, L. 2022. Don’t call it warfare. West grapples with response to Ukraine cyber aggressions. In *Politico*, 2022; NYT. 2022. Are we ready for Putin’s cyber war? In *The New York Times*, 2022.

[10] Pokročilá trvalá hrozba (Advanced Persistent Threat - APT) je pojem z odboru počítačovej bezpečnosti. Popisuje nenápadného útočníka, zvyčajne národný štát alebo štát sponzorovanú skupinu, ktorá s vynaložením veľkej časti ľudských a finančných zdrojov využíva nepoužitý prístup k počítačom. V poslednej dobe sa tento termín vzťahuje aj na neštátne skupiny, ktoré prevádzajú rozsiahly cielený prístup za konkrétnymi cieľmi. Ciele týchto útokov, ktoré sa veľmi starostlivo vyberajú a skúmajú, zvyčajne zahŕňajú veľké podniky alebo vládne siete. Dôsledky takýchto prienikov sú rozsiahle a zahŕňajú: krádež duševného vlastníctva (napr. obchodné tajomstvá alebo patenty), citlivé informácie (napr. súkromné údaje zamestnancov a používateľov), sabotáž kritických organizačných infraštruktúr (napr. vymazanie databázy), celkové prevzatie stránok atď. Vykonanie útoku APT vyžaduje viac zdrojov ako útok štandardnej webovej aplikácie. Páchatelia sú zvyčajne tímy skúsených kyberzločincov, ktorí majú značné finančné zabezpečenie. Niektoré útoky APT sú financované vládou a používané ako kybernetické vojnové zbrane.

pôsobiť skôr „geopoliticky“, či už s cieľom spôsobiť cielené prerušenia alebo so širším strategickým zámerom, ktorý kombinuje oportunistické a starostlivo prispôsobené kampane. Ich operácie siahajú od útokov na dodávateľské reťazce a ďalšie ekonomické subjekty cez ohrozenie sietí Svetovej antidopingovej agentúry (World Anti-Doping Agency – WADA) a Organizácie pre zákaz chemických zbraní (Organisation for the Prohibition of Chemical Weapons – OPCW) v októbri 2018, až po operácie „hack-and-leak“[11] a politické zásahy proti demokratickým inštitúciám (napríklad nemeckému Bundestagu v roku 2015) a procesom (napríklad voľbám v USA v roku 2016 a 2020 a vo Francúzsku v roku 2017) a rozsiahle dezinformačné kampane prostredníctvom sociálnych médií na celom svete.

Ruským kybernetickým „medveďom“ sa všeobecne pripisuje vysoký stupeň technickej vyspelosti a vynaliezavosti, zameranie sa na strategické ciele (vrátane energetickej a informačnej infraštruktúry štátu a vojenských systémov velenia a riadenia), pozoruhodná schopnosť vytvárať zmätok a modelovať nové spôsoby vykonávania starých vecí[12] – aj keď stále v kontexte kyberpriestoru tak, ako ho poznáme. V tejto súvislosti sa zdá, že Moskva toleruje (a príležitostne aj využíva) hackerov, ktorí operujú z Ruska pod podmienkou, že nekonajú proti Rusku, ale iba (alebo predovšetkým) proti záujmom Západu alebo iných aktérov. S najväčšou pravdepodobnosťou ale nie je sama, kto to robí.

Na porovnanie a na rozdiel od toho sa čínske štátne a štátom sponzorované APT (často označované ako „Pandy“) dlho sústreďovali na kybernetickú špionáž zameranú hlavne na komerčný zisk (prostredníctvom krádeže duševného vlastníctva), neskôr nasledovala akvizícia aktív a kontrola sietí (najskôr pozdĺž tzv. Novej hodvábnej cesty a potom na celom svete). Čína sa však výslovne zameriava nielen na komplexnú technologickú prevahu v strednodobom horizonte, ale aj na (re)formovanie kyberpriestoru a internetu.[13] Čínsky „model“ sa na rozdiel od stále dominantného „kalifornského“ modelu sústreďuje na takzvaný Great Firewall doma a technologickú kontrolu v zahraničí. Spolieha sa na obrovské zdroje pracovnej sily a úzku koordináciu medzi štátnymi orgánmi a súkromnými spoločnosťami, čím potenciálne ohrozuje kybernetickú nadradenosť USA a podporuje „bipolárny“ kybernetický priestor[14] alebo dokonca „Splinternet“.[15]

---

[11] Bližšie pozri: SHIRES, J. 2022. Damaging the opponent ‘the new way’: Understanding the tactics behind hack-and-leak operations. In *Atlantisch Perspectief*, 2020.

[12] Bližšie pozri: RID, T. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York : Picador, 2021; alebo GREENBERG, A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. New York : Doubleday, 2019.

[13] WOO, J. et al. 2020. National Cyber Power Index 2020. In *The Belfer Center for Science and International Affairs, Harvard University*, 2020

[14] CRABTREE, J. et al. 2021. Report launch: 'Cyber Capabilities and National Power: A Net Assessment'. In *International Institute for Security Studies*, 2021.

[15] Spinternet je opakom internetu. Spinternet je myšlienka, že otvorený, globálne prepojený internet, ktorý všetci používame, sa rozpadá na zhluk izolovaných sietí kontrolovaných vládami alebo korporáciami. Bližšie pozri: IS. Splinternet. In *Internet Society*, 2022.

Pokiaľ ide o prebiehajúci konflikt na Ukrajine, v tejto fáze je takmer nemožné urobiť presvedčivé hodnotenia o tom, čo sa presne odohráva z prísne kybernetického hľadiska. Samotná povaha kybernetickej „zbrane“ – spolu s logikou vojnovej komunikácie, ktorá má tendenciu skrývať alebo bagatelizovať neúspechy – sťažuje presné určenie toho, aké operácie boli spustené a aký dopad mohli mať. Na takomto (obmedzenom) základe sa zdá byť legitímne tvrdiť, že Rusko reálne vykonávalo nepriateľské kybernetické operácie pred konfliktom a vykonáva ich aj počas neho, ale v menšom rozsahu a s menším vplyvom, ako sa pôvodne očakávalo.[16]

Už niekoľko hodín pred inváziou a hneď po nej ruskí kybernetickí aktéri zjavne nasadili deštruktívny malvér proti rôznym cieľom na Ukrajine vrátane bankových služieb, civilnej komunikačnej infraštruktúry a vojenských veliteľských a riadiacich centier. Veľká kybernetická sabotážna operácia odstavila satelit KA-SAT, ktorý vlastní spoločnosť ViaSat – poskytovateľ vysokorýchlostných širokopásmových služieb využívaných nielen armádou, spravodajskými a policajnými jednotkami Ukrajiny, ale aj inými štátmi (vrátane mnohých krajín EÚ a NATO), pričom početné znehodnotenia webových stránok a útoky odmietnutia služby brzdili schopnosť okamžitej reakcie ukrajinských štátnych orgánov. Aj keď tieto akcie nepredstavovali až takú ohromujúcu kybernetickú ofenzívu typu „šok a hrôza“, ktorú niektorí predpovedali, boli dôkladne vopred pripravené, pretože si vyžadovali systematické prieniky a využívanie existujúcich zraniteľností. Je zrejmé, že boli naplánované tak, aby sa zhodovali s počiatočným kinetickým úsilím o ovládnutie Kyjeva v priebehu niekoľkých dní. Dnes je už takmer isté, že Moskva si predstavovala rýchle vojenské víťazstvo, a preto nevidela potrebu (alebo užitočnosť) masívnych kybernetických útokov. Navyše, americké obranné operácie v kyberpriestore zabránili ďalším ruským útokom narušiť železničné siete, ktoré sa používali na prepravu vojenských zásob a na pomoc miliónom ukrajinských občanov pri evakuácii.[17]

Všetky tieto uvedené faktory pravdepodobne prispeli k zmierneniu účinkov ruských nepriateľských kybernetických aktivít na Ukrajine do takej miery, že niektorí začali uvažovať o tom, či ruská kybernetická „sila“ nebola preceňovaná.[18] Ruskí kybernetickí bojovníci sa určite na „špeciálnej vojenskej operácii“ realizovanej Kremľom podieľali a urobili tak v rámci počiatočného „hybridného“ vojnového plánu, ktorého zjavné nedostatky pravdepodobne neboli zapríčinené ich vinou alebo chybou. V skutočnosti je rozsah a intenzita ich úsilia značná a môže sa stále zintenzívňovať a diverzifikovať, ak bude konflikt aj naďalej pokračovať.

---

[16] Bližšie pozri: MANJOO, F. The Ukrainian cyberwar that never materialized. In *The New York Times*, 2022; alebo LANDON, G. The digital war that wasn’t, yet. Cyber-attacks on Ukraine are conspicuous by their absence. In *The Economist*, 2022.

[17] CATTLER, D. – BLACK, D. The Myth of the Missing Cyberwar. Russia’s Hacking Succeeded in Ukraine And Poses a Threat Elsewhere, Too. In *Foreign Affairs*, 2022.

[18] SRIVASTAVA, E. M. 2022. Kremlin’s cyber abilities may be overhyped, says UK spy chief. In *Financial Times*, 2022.

To znamená, že očakávania a predpovede o možnom rozsahu a vplyve samostatných kybernetických operácií na konflikt mohli byť trochu prehnané, keďže kybernetické „zbrane“ zatiaľ stále slúžia najmä ako pomocné taktické nástroje v rámci širšej politickej stratégie a vojenského ťaženia.[19] Na druhej strane je potrebné v súvislosti s ruskou agresiou na Ukrajine poznamenať, že kybernetické útoky a zákerné aktivity (tiež „hybridného“ charakteru) proti krajinám a vládam, ktoré podporujú Ukrajinu, od februára eskalovali a vážne testujú odolnosť európskych hospodárskych a politických štruktúr.

KYBERNETICKÁ BEZPEČNOSŤ A OBRANA EURÓPSKEJ ÚNIE

Keď predsedníčka Európskej komisie Ursula von der Leyenová počas svojho prejavu o stave Únie v Európskom parlamente v roku 2021[20] oznámila zámer EÚ vypracovať politiku kybernetickej bezpečnosti a obrany ako súčasť svojej digitálnej agendy[21], úradníci Európskej služby pre vonkajšiu činnosť (ESVČ)) premýšľali, čo presne má na mysli. Čoskoro sa ukázalo, že mala na mysli širší postoj Európskej únie v oblasti kybernetickej odolnosti. Takáto zámena medzi kybernetickou obranou a kybernetickou bezpečnosťou však nie je nezvyčajná. Hoci neexistuje žiadna jednotná, unifikovaná a všeobecne akceptovaná definícia, kybernetická bezpečnosť zahŕňa – všeobecne povedané – opatrenia na ochranu kybernetického priestoru pred akýmikoľvek nepriateľskými aktivitami. Tých je postupom času stále viac, preto má v súčasnosti každá väčšia firma, podnik, organizácia, verejná inštitúcia a/alebo medzinárodný orgán špecializovaných pracovníkov zodpovedných za ochranu ich sietí pred neoprávneným prienikom zvonku.

Kybernetická obrana sa týka skôr tých opatrení, zariadení a štruktúr, ktoré sú v kompetencii armády alebo nejakým spôsobom zasahujú do vojenských aktivít a spôsobilostí (napríklad spravodajstva a pod.). Kybernetická obrana sa však môže ako pojem použiť aj všeobecnejšie, a to na vyjadrenie akcie, a nie na zapojenie konkrétneho aktéra. V každom prípade, rôzne definície odrážajú rôzne mandáty s mnohými rozdielmi medzi vládami aj štátmi. V dôsledku toho posilnenie kybernetickej „obrany“ nemusí nevyhnutne zahŕňať zapojenie (iba) armády.[22] Dôležité je, že takéto reakcie nemusia byť obmedzené iba na kybernetickú doménu, naopak, viaceré národné stratégie (prijaté v posledných rokoch) odkazujú aj na diplomatické, informačné, vojenské, ekonomické, finančné, spravodajské a právne opatrenia[23] (DIMEFIL –

---

[19] RID, T. 2022. Why you haven’t heard about the secret cyberwar in Ukraine. In *The New York Times*, 2022.

[20] Európska komisia. 2021. 2021 State of the Union Address by President von der Leyen. In *European Commission Press Corner*, 2022.

[21] Bližšie pozri: Európsky parlament. 2022. Digital Agenda for Europe. In *European Parliament – Fact Sheets on the European Union*, 2022.

[22] MISSIROLI, A. 2019. The Dark Side of the Web: Cyber as a Threat. In *European Foreign Affairs Review*, 2019, roč. 24. č. 2, s. 135-152

[23] Bližšie pozri: KIMSEY, D. et al. 2020. Utilization of the DIMEFIL Framework in a Case Study Analysis of Security Cooperation Success. In *Small Wars Journal*, 2020.

Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement) ako súčasť komplexného súboru nástrojov pre viaceré domény.

Z tohto hľadiska sa EÚ aj Severoatlantická aliancia (ďalej len „NATO“) vyzbrojili, aby zabránili nepriateľským kybernetickým aktivitám voči svojim orgánom, štruktúram a členským štátom, zmiernili ich a reagovali na ne, a to budovaním svojich silných stránok a mandátov. EÚ posilnila svoju kybernetickú odolnosť tým, že sa uchýlila k svojim regulačným právomociam a odsúhlasila novú legislatívu zameranú na posilnenie odolnosti kritických subjektov a informačnej infraštruktúry, počnúc smernicou o sieťových a informačných systémoch[24] (NIS Directive) a stratégiou EÚ v oblasti kybernetickej bezpečnosti[25] (EU Cyber Security Strategy), obe aktualizované v r. 2020. Svoju zahraničnopolitickú odozvu zlepšila aj vďaka špeciálnemu súboru kybernetických diplomatických nástrojov[26] (EU Cyber Direct), ktorý bol spustený v roku 2019 a ktorý umožňuje uvaliť sankcie voči jednotlivcom a subjektom v prípade závažných kybernetických útokov.

NATO prijalo prísnejšie technické kritériá pre vojenské siete a posilnilo svoje základné požiadavky na zabezpečenie odolnosti kritickej národnej infraštruktúry. Aliancia zároveň odsúhlasila v roku 2019 príručku pre možnosti strategickej reakcie na významné škodlivé kybernetické aktivity, to znamená tie, ktoré sú pod úrovňou ozbrojeného konfliktu, vytvorila mechanizmus na integráciu niektorých útočných kybernetických nástrojov do svojich operácií a misií – tzv. Suverénne kybernetické efekty poskytované dobrovoľne spojencami (Sovereign Cyber Effects Provided Voluntarily by Allies – SCEPVA)[27]. Na summite NATO v Bruseli v roku 2021 spojenci schválili novú komplexnú politiku kybernetickej obrany, ktorá podporuje tri základné úlohy NATO, ktorými sú kolektívna obrana, krízový manažment a kooperatívna bezpečnosť, ako aj jeho celkové odstrašovanie a obranný postoj.[28]

V neposlednom rade, okrem regulácie EÚ a štandardizácie NATO, počítačové tímy reakcie na incidenty oboch organizácií – CERT-EU[29] a N-CIRC[30] – podpísali bilaterálnu technickú dohodu o výmene informácií o aktéroch hrozieb,[31] Od februára 2016 sa kybernetické prvky pravidelne začleňujú do cvičení krízového manažmentu, na ktorých sa podieľa Únia aj

---

[24] Bližšie pozri: ENISA. 2020. NIS Directive. In *European Union Agency for Cyber Security*, 2020.

[25] Bližšie pozri: Európska komisia. 2020. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. In *European Commission Press Corner*, 2020.

[26] EU Cyber Direct – Iniciatíva EÚ, ktorá podporuje kybernetickú diplomaciu a medzinárodné digitálne záväzky Európskej únie s cieľom posilniť poriadok založený na pravidlách v kybernetickom priestore a budovať kyberneticky odolné spoločnosti. S týmto cieľom sa vykonáva výskum, podporuje budovanie kapacít v partnerských krajinách a podporuje spolupráca viacerých zainteresovaných strán. Bližšie pozri: EUCD. EU Cyber Diplomacy Initiative. In *EU Cyber Direct*, 2022.

[27] GOŹDZIEWICZ, W. 2019. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). In *Cyber Defence Magazine*, 2019.

[28] CCDCOE. 2021. NATO Summit Updates Cyber Defence Policy. In *Cooperative Cyber Defence Centre of Excellence*, 2021.

[29] CERT-EU - The Computer Emergency Response Team for the EU institutions, bodies and agencies (Tím pre počítačovú pohotovosť pre inštitúcií, orgánov a agentúr EÚ). Bližšie pozri: EU. CERT-EU. In *CERT-EU, 2022*

[30] NATO. 2022. NATO Cyber Security Centre. In *NCI Agency*, 2022.

[31] EEAS. 2020. EU and NATO cyber defence cooperatione. In *European Union External Action*, 2020.

Aliancia, a prostredníctvom špecializovaných agentúr a centier výnimočnosti boli vyvinuté nové vzdelávacie platformy. Zdieľanie spravodajských informácií v oblasti kybernetiky a budovanie kapacít s partnerskými krajinami (vrátane Ukrajiny) sa tiež výrazne prehĺbilo a prebieha medzi vládnymi agentúrami viac-menej neformálne.

Ruská invázia na Ukrajinu k tomu všetkému pridala ďalšiu naliehavosť. Strategický kompas EÚ[32] schválený koncom marca, ako aj nová Strategická koncepcia NATO[33] schválená koncom júna 2022 zdôrazňujú čoraz viac „sporný" charakter kybernetického priestoru a prenikanie strategickej konkurencie do digitálnej sféry. Rusko pôsobí ako priama „hrozba" a Čína ako rastúca „výzva". Obidva dokumenty tiež vyzývajú svoje členské štáty k tomu, aby posilnili bezpečnú komunikáciu, pripravenosť a odolnosť, ako aj ich zlepšili ich postoj voči kybernetickým útokom.

Konkrétnejšie, Strategický kompas EÚ začleňuje kybernetické útoky zo strany štátnych a neštátnych subjektov ako súčasť širšieho hodnotenia nekonvenčných hrozieb, medzi ktoré zahŕňa aj hybridné stratégie, dezinformačné kampane, politické zasahovanie, ekonomický nátlak a inštrumentalizáciu migrácie štátnymi a neštátnymi subjektmi. Pokiaľ ide o reakciu, Únia sa zaväzuje posilniť kybernetickú bezpečnosť (okrem iného cestou zákona o kybernetickej odolnosti) a aj naďalej rozvíjať politiku kybernetickej obrany zvýšením spolupráce medzi EÚ a vnútroštátnymi aktérmi kybernetickej obrany (vrátane vojenských). Rovnako tak aj s ďalšími podobne zmýšľajúcimi partnermi, predovšetkým s NATO, a to posilnením kapacít kybernetického spravodajstva. Strategická koncepcia NATO zasa uznáva, že EÚ je jedinečným a základným partnerom NATO a že obe organizácie realizujú doplnkové, koherentné a vzájomne sa posilňujúce úlohy aj v boji proti kybernetickým a hybridným hrozbám.

Opatrenia, ktoré doteraz prijali jednotlivé európske krajiny, ako aj EÚ a NATO v reakcii na nepriateľské kybernetické aktivity namierené proti ich sieťam, orgánom a štruktúram, nemusia predstavovať strategické odstrašovanie, ako ho poznáme, t. j. klasická kombinácia odmietnutia a trestu (pretože v jadrovej oblasti zbrane nie sú určené na použitie, ale len na odstrašenie, zatiaľ čo v kybernetickej oblasti sa používajú neustále). Napriek tomu môžu prispieť k prispôsobenému odstrašovaniu: a) vhodnou kombináciou vyššieho stupňa popierania (odolnosť), sklonu odhaľovať a stigmatizovať nepriateľskú činnosť v rámci kybernetickej domény, b) neustálym prispôsobovaním obrany vlastnej zraniteľnosti a typu zainteresovaných aktérov hrozby, a c) zodpovedajúcim spôsobom kalibrovať odozvy a konať spoločne.[34]

---

[32] Európska rada. A Strategic Compass for a stronger EU security and defence in the next decade. In *European Council*, 2022.

[33] NATO. NATO 2022 Strategic Concept. In *NATO Info*, 2022.

[34] CCDCOE. 2021. EU Cyber Defence Policy Framework Presents More Than 40 Action Measures. In *Cooperative Cyber Defence Centre of Excellence*, 2021.

ZÁVER

Záverom je možné konštatovať, že kybernetická bezpečnosť a kybernetická obrana zahŕňajú celý rad civilných a vojenských akcií, aktivít, koncepcií, stratégií, orgánov a zdrojov, ktoré si vyžadujú vysoký stupeň koordinácie, konvergencie a konzistentnosti na národnej aj nadnárodnej úrovni. Ani EÚ, ani NATO nedisponujú všetkými potrebnými nástrojmi a kompetenciami, čo ich podporuje spolupracovať medzi sebou, ako aj v kybernetickej doméne s nenahraditeľným súkromným sektorom a vzájomne sa dopĺňať. Všetky spoločné vyhlásenia, ktoré vydali vedúci predstavitelia oboch organizácií od roku 2016, to veľmi jasne uvádzajú a odzrkadľujú sa vo vzájomnej spolupráci.

Na druhej strane, kybernetická bezpečnosť aj kybernetická obrana zostávajú primárne a prevažne národnými výsadami s minimálnym alebo podmieneným delegovaním právomocí na nadnárodné alebo multilaterálne orgány aj v porovnaní s inými (civilnými či dokonca aj vojenskými) oblasťami. Zároveň sú v prenesenom slova zmysle základnými kolektívnymi športami, kde jednotlivé tímy sú také silné, ako sú silní ich najslabší hráči (niektorí sú určite zraniteľnejší ako iní) a kde sú konzultácie a spolupráca cez hranice a medzi jurisdikciami životne dôležité.

V skutočnosti sa doteraz nadnárodné konzultácie a medzinárodná spolupráca v tejto oblasti uskutočňovali väčšinou multi-bilaterálne, t. j. medzi jednotlivými členskými štátmi EÚ na jednej strane a USA, čiastočne Spojeným kráľovstvom (po Brexite) a ďalšími tretími krajinami (napríklad Izraelom) na strane druhej. Asymetria v schopnostiach – najmä pokiaľ ide o spravodajstvo, situačné povedomie a nástroje reakcie – je taká veľká, že potreba partnerstva s kľúčovými západnými kybernetickými „mocnosťami“ proti nepriateľským často prevýšila očakávania a požiadavky na väčšiu spoluprácu na úrovni EÚ.

Práve medzi členskými štátmi EÚ je potrebné urobiť viac – napríklad v rámci vyššie v texte spomínanej Stálej štruktúrovanej spolupráce (PESCO), kde je relevantných projektov zameraných alebo aspoň parciálne sa týkajúcich kybernetickej bezpečnosti a obrany málo a navyše majú obmedzený rozsah – s cieľom zlepšiť vlastnú kolektívnu schopnosť celého bloku fungovať a dôveryhodne spolupracovať s partnermi. V tejto oblasti treba (ešte viac ako v iných oblastiach) výzvu na väčšiu „strategickú autonómiu“ EÚ chápať skôr ako silnejší príspevok Únie k spoločnému úsiliu s rovnako zmýšľajúcimi partnermi – medzi ktorých musí patriť aj súkromný sektor, v ktorom nepôsobí veľa spoločnosti z EÚ – než ako túžbu a ambíciu fungovať samostatne. A možno nie náhodou jediná veta venovaná tomuto pojmu v novom Strategickom kompase priamo spája „strategickú autonómiu“ so „schopnosťou EÚ spolupracovať s partnermi na ochrane svojich hodnôt a záujmov“.

Politická spolupráca a konvergencia medzi rovnako zmýšľajúcimi aktérmi sú napokon nevyhnutné aj na podporu a uľahčenie globálneho úsilia zachovať slobodný, otvorený, bezpečný a stabilný kyberpriestor a odradiť (alebo aspoň obmedziť) operácie, ktoré výrazne

presahujú rámec toho, čo medzinárodné spoločenstvo považuje za prijateľné. A hoci v takej špecifickej doméne, akou je kybernetická, ruská invázia na Ukrajinu nemusela priniesť tzv. bod zlomu alebo Zeitenwende[35] (ako to nazval nemecký spolkový kancelár Olaf Scholz po ruskom vpáde na Ukrajinu), poskytla však ďalší dôležitý impulz pre koordináciu politík na úrovni EÚ aj mimo nej a zdôraznila strategický význam digitálnej sféry pre bezpečnosť a obranu Európskej únie a jej členských štátov.

Zoznam použitej literatúry a zdrojov:

BILQUIN, B. 2022. Russia's war on Ukraine: The EU's financing of military assistance to Ukraine. In *European Parliamentary Research Centre*, 2022. Dostupné na internete: <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)729436>.

BLACKWILL, R. D. 2020. The U.S. Pivot to Asia and American Grand Strategy. In *Council on Foreign Relations*, 2018. [online] [cit. 1.12.2022] Dostupné na internete: <https://www.cfr.org/project/us-pivot-asia-and-american-grand-strategy>.

CATTLER, D. – BLACK, D. 2022. The Myth of the Missing Cyberwar. Russia's Hacking Succeeded in Ukraine And Poses a Threat Elsewhere, Too. In Foreign Affairs, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.

CCDCOE. 2021. EU Cyber Defence Policy Framework Presents More Than 40 Action Measures. In *Cooperative Cyber Defence Centre of Excellence*, 2021. [online] [cit. 13.12.2022] Dostupné na internete: <https://ccdcoe.org/incyder-articles/eu-cyber-defence-policy-framework-presents-more-than-40-action-measures/>.

CCDCOE. 2021. NATO Summit Updates Cyber Defence Policy. In *Cooperative Cyber Defence Centre of Excellence*, 2021. [online] [cit. 13.12.2022] Dostupné na internete: <https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/>.

CERULUS, L. 2022. Don't call it warfare. West grapples with response to Ukraine cyber aggressions. In *Politico*, 2022. [online] [cit. 11.12.2022] Dostupné na internete: <https://www.politico.eu/article/cyber-security-russia-ukraine-nato-europe/>.

CRABTREE, J. et al. 2021. Report launch: 'Cyber Capabilities and National Power: A Net Assessment'. In *International Institute for Security Studies*, 2021. [online] [cit. 11.12.2022] Dostupné na internete: <https://www.iiss.org/events/2021/06/cyber-capabilities-report-launch>.

[35] Zeitenwende = Bod zlomu; koniec jednej epochy (éry) a začiatok novej epochy (éry)

EDA. 2022. European Defence Fund. In *European Defence Agency*, 2022. [online] [cit. 28.11.2022] Dostupné na internete: <https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)>.

EDA. 2022. Permanent Structured Cooperation. In *European Defence Agency*, 2022. [online] [cit. 28.11.2022] Dostupné na internete: <https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO)>.

EEAS. 2020. EU and NATO cyber defence cooperatione. In *European Union External Action*, 2020. [online] [cit. 13.12.2022] Dostupné na internete: <https://www.eeas.europa.eu/node/3667_en>.

EEAS. 2022. Military Planning and Conflict Capability. In *European Union External Action*, 2022. [online] [cit. 28.11.2022] Dostupné na internete: <https://www.eeas.europa.eu/eeas/military-planning-and-conduct-capability-mpcc_en>.

ENISA. 2022. NIS Directive. In *European Union Agency for Cyber Security*, 2022. [online] [cit. 13.12.2022] Dostupné na internete: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>.

EU. 2022. CERT-EU. In *CERT-EU*, 2022. [online] [cit. 13.12.2022] Dostupné na internete: <https://cert.europa.eu>.

EUCD. 2022. EU Cyber Diplomacy Initiative. In *EU Cyber Direct*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://eucyberdirect.eu>.

Európska komisia. 2020. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. In *European Commission Press Corner*, 2020. [online] [cit. 12.12.2022] Dostupné na internete: <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_239>.

Európska komisia. 2021. 2021 State of the Union Address by President von der Leyen. In *European Commission Press Corner*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701>.

Európska komisia. 2022. European Peace Facility. In *European Commission – Service for Foreign Policy Instruments*, 2022. [online] [cit. 27.11.2022] Dostupné na internete: <https://fpi.ec.europa.eu/what-we-do/european-peace-facility_en>.

Európska rada. 2022. A Strategic Compass for a stronger EU security and defence in the next decade. In *European Council*, 2022. [online] [cit. 28.11.2022] Dostupné na: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>.

Európska rada. 2022. A Strategic Compass for a stronger EU security and defence in the next decade. In *European Council*, 2022. [online] [cit. 13.12.2022] Dostupné na internete:

<https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>.

Európska rada. 2022. EU sanctions against Russia explained. In *European Council*, 2022. [online] [cit. 29.11.2022] Dostupné na internete: <https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/>.

Európsky parlament. 2022. Digital Agenda for Europe. In *European Parliament – Fact Sheets on the European Union*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe>.

FIOTT, D. 2018. Strategic autonomy: towards 'European sovereignty' in defence? In *European Union Institute for Security Studies*, 2018. [online] [cit. 28.11.2022] Dostupné na internete: <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2012_ _Strategic%20Autonomy.pdf>.

GOŹDZIEWICZ, W. 2019. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). In *Cyber Defence Magazine*, 2019. [online] [cit. 13.12.2022] Dostupné na internete: <https://www.cyberdefensemagazine.com/sovereign-cyber/>.

GREENBERG, A. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York : Doubleday, 2019. 368 s. ISBN 978-0-385-54441-2.

IS. 2022. Splinternet. In *Internet Society*, 2022. [online] [cit. 11.12.2022] Dostupné na internete: <https://www.internetsociety.org/splinternet/>.

KIMSEY, D. et al. 2020. Utilization of the DIMEFIL Framework in a Case Study Analysis of Security Cooperation Success. In *Small Wars Journal*, 2020. [online] [cit. 12.12.2022] Dostupné na internete: <https://smallwarsjournal.com/jrnl/art/utilization-dimefil-framework-case-study-analysis-security-cooperation-success>.

LANDON, G. 2022. The digital war that wasn't, yet. Cyber-attacks on Ukraine are conspicuous by their absence. In *The Economist*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>.

MANJOO, F. 2022. The Ukrainian cyberwar that never materialized. In The New York Times, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.nytimes.com/2022/03/11/opinion/russia-ukraine-cyberattacks.html>.

MISSIROLI, A. 2019. The Dark Side of the Web: Cyber as a Threat. In *European Foreign Affairs Review*, 2019. roč. 24. č. 2, s.135-152. ISSN 1384-6299.

NATO. 2022. NATO 2022 Strategic Concept. In *NATO Info*, 2022. [online] [cit. 13-12-2022] Dostupné na internete: <https://www.nato.int/strategic-concept/>.

NATO. 2022. NATO Cyber Security Centre. In *NCI Agency*, 2022. [online] [cit. 13.12.2022] Dostupné na internete: <https://www.ncirc.nato.int>.

NYT. 2022. Are we ready for Putin's cyber war? In *The New York Times*, 2022. [online] [cit. 11.12.2022] Dostupné na internete: <https://www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html>.

RID, T. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York : Picador, 2020. 528 s. ISBN 978-1-2507-8740-8.

RID, T. 2022. Why you haven't heard about the secret cyberwar in Ukraine. In *The New York Times*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html>.

SHIRES, J. 2022. Damaging the opponent 'the new way': Understanding the tactics behind hack-and-leak operations. In *Atlantisch Perspectief*, 2020, roč. 44, č. 4 (Special Edition: Uncovering an unseen nemesis), s. 20-25. ISSN 2667-3479.

SRIVASTAVA, E. M. 2022. Kremlin's cyber abilities may be overhyped, says UK spy chief. In *Financial Times*, 2022. [online] [cit. 12.12.2022] Dostupné na internete: <https://www.ft.com/mehul-srivastava?page=2>.

WOO, J. et al. 2020. National Cyber Power Index 2020. In *The Belfer Center for Science and International Affairs*, *Harvard University*, 2020. [online] [cit. 11.12.2022] Dostupné na internete: <https://www.belfercenter.org/publication/national-cyber-power-index-2020>.