O KYBERNETICKEJ DIMENZII BOJISKA

ON THE CYBER DIMENSION OF THE BATTLEFIELD

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 North Atlantic Alliance, since its summit held in July 2016 in Warsaw, Poland, has considered cyberspace to be an area of operations. Cyberspace, whether in the form of a simple computer connected to the Internet or several interconnected and connected computers or even high-performance modern servers, is now a vital space for the security and defence of any state or grouping (alliance, pact, union) of states. Therefore, to ensure its security and defence, the North Atlantic Alliance not only strengthens common, collective cyber capabilities, but also supports its member states in strengthening their own, individual cyber capabilities and capabilities so that they can respond effectively and efficiently to current, existing, and potential possible future cyber threats. The author therefore deals with these threats, vulnerabilities, and risks in the article; and at the same time, using relevant methods of interdisciplinary scientific research, it explores cyberspace as one of the dimensions of the current battlefield.

Keywords: cyberspace, cyber threats, security, defence, vulnerability, battlefield.

Abstrakt:

Severoatlantická aliancia, od svojho samitu, ktorý sa konal v júli v roku 2016 vo Varšave v Poľsku, považuje kybernetický priestor za operačný priestor. Kybernetický priestor, či už v podobe jednoduchého počítača pripojeného k internetu alebo viacerých vzájomne prepojených a pripojených počítačov či dokonca vysoko výkonných moderných serverov, predstavuje v súčasnosti životne dôležitý priestor pre bezpečnosť a obranu akéhokoľvek štátu či zoskupenia (aliancie, paktu, únie) štátov. Preto Severoatlantická aliancia, v záujme zaistenia svojej bezpečnosti a obrany, posilňuje nielen spoločné, kolektívne kybernetické spôsobilosti, ale zároveň podporuje jej členské štáty v posilňovaní ich vlastných, individuálnych kybernetických schopností a kapacít, aby mohli efektívne a účinne reagovať na súčasné, existujúce i potenciálne možné budúce kybernetické hrozby. Autor sa z toho dôvodu zaoberá v článku práve týmito hrozbami, zraniteľnosťami a rizikami; a súčasne, s využitím relevantných metód interdisciplinárneho vedeckého výskumu, skúma kybernetický priestor ako jednu z dimenzií súčasného bojiska.

Kľúčové slová: kybernetický priestor, bezpečnosť, obrana, zraniteľnosť, bojisko.

Úvod

V súčasnom období stále dominantnejšieho postavenia informačných a komunikačných technológií (ďalej len „IKT“) vo viacerých sférach života ľudskej spoločnosti sa kybernetický priestor stal pre vlády štátov na celom svete veľmi závažným bezpečnostným problémom a viedol ich k prijatiu veľkého množstva opatrení na zvýšenie kybernetickej bezpečnosti.[1] Vývoj v posledných rokoch potvrdzuje, že masívne zavádzanie a spoliehanie sa na IKT postupne viedlo k mnohým bezpečnostným problémom. Vlády štátov preto začali vyvíjať postupy, prijímať opatrenia a realizovať viaceré kroky na ochranu kybernetického priestoru pred kybernetickými útokmi. Kybernetická bezpečnosť a obrana sa stala jednou z najvyšších vládnych priorít v prevažnej väčšine krajín sveta.

Mnoho vrcholných predstaviteľov vlád štátov v tejto súvislosti uznalo, že ochranu spoločnosti proti kybernetickým útokom a ďalším nežiaducim a škodlivým kybernetickým aktivitám možno úspešne riešiť iba prostredníctvom medzinárodnej spolupráce a partnerstva. Najrozvinutejšia je táto spolupráca na úrovni Severoatlantickej aliancie (ďalej len „NATO“ alebo „Aliancia“), čo je nakoniec aj absolútne logické, keďže ide o vojenské-politické zoskupenie štátov založené a fungujúce s primárnym cieľom zaistenia vzájomnej (kolektívnej) obrany a spoločných bezpečnostných záujmov.

Technologický pokrok, predovšetkým v už spomínanej oblasti IKT, ktorého sme svedkami v posledných desaťročiach, priniesol nové možnosti prenosu a podávania informácií a významným spôsobom ovplyvnil rozhodovací proces (nielen) v NATO. Takýto vývoj a stav má, pochopiteľne, svoje pozitívne, ale aj negatívne stránky, ktoré sa prejavujú najmä vo vyššej zraniteľnosti súvisiacej s ochranou infraštruktúry, ktorá umožňuje spoľahlivé a efektívne riadenie informácií, tzv. informačný manažment. V nadväznosti na už naznačený prudký technologický pokrok sa zrodilo nové operačné prostredie, nový priestor → kybernetický priestor (ďalej len „kyberpriestor“), v ktorom účinky realizovaných aktivít, resp. prebiehajúcich akcií majú stále väčší vplyv na schopnosť fungovania vo fyzickom prostredí.

Zvýšenú dôležitosť a význam kyberpriestoru vo sfére zaistenia bezpečnosti a obrany potvrdzujú aj nedávne vyhlásenia generálneho tajomníka NATO Jensa Stoltenberga, ktorý uviedol, že operácie v kybernetickom priestore by mali byť rovnako účinné ako pozemné, námorné a vzdušné operácie, pretože každá súčasná kríza či konflikt majú svoju kybernetickú dimenziu. Na zdôraznenie svojich predchádzajúcich slov dodal: „*V kybernetickom priestore musíme byť rovnako silní a efektívni ako na súši, na mori a vo vzduchu*.“[2]

V tejto súvislosti je potrebné uviesť, že úspech spoločných operácií závisí od integrácie všetkých silových prvkov zapojených do vybudovania koherentnej jednotky. Táto integrácia zaisťuje koordináciu a synchronizáciu realizovaných akcií všetkých silových prvkov, a to podľa priorít stanovených pre danú operáciu. Pretože manažment bojového priestoru (ďalej len

[1] Bližšie pozri: HROMADA, M. 2017. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133
[2] NATO. 2018. NATO Calls On Taliban To Join Ceasefire. In *ForcesNet*, 2018.

„bojisko“) je považovaný za kľúčový prvok spoločných operácií, poznanie jednotlivých komponentov a prvkov na bojisku a spôsob ich interakcie je potrebný pre všetkých aktérov, ktorí zdieľajú rovnaký operačný priestor.

Aj preto je primárnym cieľom autora článku, využijúc viaceré relevantné metódy interdisciplinárneho vedeckého výskumu (najmä analyticko-syntetickú metódu, obsahovú a kvalitatívnu analýzu, analýzu štúdia dokumentov atď.), nadväzujúc na práce renomovaných zahraničných i domácich autorov z oblasti bezpečnosti a zvlášť zo sféry kybernetickej bezpečnosti (Smeetsa[3], Van Haastera[4], Sigholma[5], Singera a Friedmana[6], Hromadu[7], Lukáša[8], Korauša[9], Gregu[10], Fabiána[11], Kazanského[12], Kollára[13], Valucha[14], Andrassyho[15] a ďalších) a vychádzajúc z dostupných informácií a aspektov týkajúcich sa kybernetických operácií v kybernetickom priestore, čiže z ich konceptu, štruktúry a účinkov a tiež toho, ako Aliancia a jej členské štáty kladú dôraz na rozvoj kybernetických spôsobilostí v rámci zaistenia kybernetickej bezpečnosti, a zároveň poukázať prostredníctvom tohto vedeckého výskumu na kybernetický priestor ako na jednu z dimenzií bojového priestoru, v ktorom permanentne prebiehajú ofenzívne i defenzívne kybernetické operácie.

---

[3] SMEETS, M. Organizational integration of offensive cyber capabilities: A primer on the benefits and risks. In *9th International Conference on Cyber Conflict (CyCon)*. Tallinn : IEEE, 2017

[4] Van HAASTER, J. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019

[5] SIGHOLM, J. Non-State Actors in Cyberspace Operations. In Journal of Military Studies, 2016, roč. 4, č. 1

[6] SINGER, P. W. – FRIEDMAN, A. Cybersecurity and Cyberwar (What Everyone Needs to Know®). Oxford : Oxford University Press, 2014

[7] HROMADA, M. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I*. Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133

[8] LUKÁŠ, L. a kol. *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017.

[9] KORAUŠ, A. – KELEMEN P. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Fakulta medzinárodných vzťahov Ekonomickej univerzity. Bratislava : Vydavateľstvo Ekonóm, 2018

[10] GREGA, M. – ŽENTEK, M. – NEČAS, P. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. Krakow : Apeiron University of Public and Individual Security in Kraków, 2020, s. 172-229

[11] FABIÁN, M. – MINTÁL, J. M. – UŠIAK, J. EU Security Threats Resulting from Disinformation in Cyberspace. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. Krakow : Apeiron University of Public and Individual Security in Kraków, 2020, s. 116-139

[12] KAZANSKÝ, R. Conflict in cyberspace - framework of definitions. In Fabián, K. - Beňuška, T. (eds*.): Analysis of Social Network Security. Threats in cyberspace*. Krakow : Apeiron University of Public and Individual Security in Kraków, 2020, s. 32-68.

[13] KOLLÁR, D. Current Trends and Challenges in the Cyberspace and Cyber Security. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*.. Krakow : Apeiron University of Public and Individual Security in Kraków, 2020, s. 10-31

[14] VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava : Wolters Kluwer, 2019

[15] ANDRASSY, V. – GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18

Dimenzie bojiska

Bojisko (bojový priestor) zahŕňa všetky aspekty v oblasti spoločných operácii, pri ktorých dochádza k vojenským akciám. Skladá sa z piatich dimenzií: a) námornej, b) pozemnej, c) vzdušnej, d) vesmírnej a e) kybernetickej. Na dimenziu je pritom potrebné sa pozerať ako na špecifický priestor so špecifickými detailmi a riadiť sa pritom špecifickými pravidlami. Žiadnu z vyššie uvedených dimenzií pritom nemožno považovať za izolovanú, pretože aktivita v jednej dimenzii môže mať dôsledky na ostatné dimenzie. Kybernetická dimenzia si vyžaduje rýchle, dynamické riadenie, aby sa naplno využili výhody technologického pokroku v oblasti informačných a komunikačných technológií. Informačný manažment totiž uprednostňuje informačnú komunikáciu a využívanie informácií v správnom čase a na správnom mieste, aby podporoval riadenie a velenie a zároveň umožňoval slobodu konania. Synchronizácia s informačnými operáciami a systémom ISR (Intelligence, Surveillance and Reconnaissance = spravodajstvo, sledovanie a prieskum) umožňuje veliteľom zvíťaziť a udržať si informačnú prevahu. Tá je generovaná operačnou výhodou vyplývajúcou zo zberu, spracovania a šírenia toku informácií a zabránením protivníkovi urobiť to isté.[16] Získanie informačnej prevahy je nevyhnutné, pretože predstavuje jeden zo základných princípov Network Centric Warfare[17], novej teórie vojny v informačnom veku, ktorá vytvára rozhodujúcu výhodu na bojisku.

Vymedzenie a definovanie kyberpriestoru

Kyberpriestor pozostáva z veľkého počtu sietí, uzlov a systémových údajov, ktoré podporujú ich správny chod. Aj keď nie sú všetky uzly a siete prepojené, existuje tendencia zvyšovať prepojenie. Siete môžu byť zámerne izolované rôznymi prístupovými protokolmi alebo fyzickým oddelením. Kým sa však dostaneme k jeho vymedzeniu a definovaniu je potrebné si najskôr vymedziť a definovať kybernetickú bezpečnosť, ktorá sa, aj v nadväznosti na už spomínaný technologický pokrok, stáva stále dôležitejšou oblasťou celkového zaistenia bezpečnosti štátov, zoskupení, organizácií atď.

Jednoduchá, základná definícia kybernetickej bezpečnosti hovorí, že je to *„schopnosť chrániť kybernetický priestor pred kybernetickými útokmi“*.[18] Širšia, obsiahlejšia definícia hovorí, že *„kybernetická bezpečnosť predstavuje súhrn organizačných, politických, právnických, technických a vzdelávacích opatrení a nástrojov smerujúcich k zaisteniu chráneného a odolného kyberpriestoru pre subjekty verejného a súkromného sektora. Pomáha identifikovať, hodnotiť a riešiť hrozby v kyberpriestore, znižovať ich riziká a eliminovať dopady*

[16] U.S. DoD. 2014. *Joint Publication 3-13. Information Operations*. Washington : United States Department of Defense, 2014, s. 84.

[17] Bližšie pozri: ALBERTS, D. S. – GARSTKA, J. J. – STEIN, F. P. 2010. *Network Centric Warfare: Developing and Leveraging Information Superiority*.

[18] NIST. 2013. *Glossary of Key Information Security Terms*. Washington : United States Department of Commerce, 2013, s. 58

kybernetických útokov, ktoré sa realizujú napríklad prostredníctvom kyberterorizmu, kyberšpionáže, či kyberkriminality".[19]

Kybernetický priestor, kľúčový pojem z hľadiska obsahu tohto článku, je definovaný ako *„virtuálny priestor bez hraníc, považovaný za globálnu interaktívnu doménu v rámci informačného prostredia, ktorá je charakteristická používaním elektronického a elektromagnetického spektra pre vytváranie, ukladanie, modifikovanie a výmenu dát a využívanie služieb. Kybernetický priestor znamená aj kombinovaný fenomén globálneho prepojenia, decentralizovaných a stále sa rozširujúcich elektronických informačných, komunikačných a riadiacich systémov, ako aj prepojenia spoločenských a hospodárskych procesov objavujúcich sa vo forme dát a informácií prostredníctvom týchto systémov, vrátane dát v nich uložených, resp. spracovávaných"*.[20]

Iná definícia kybernetického priestoru hovorí, že *„ide o globálnu doménu v informačnom prostredí pozostávajúcu z vzájomne prepojenej siete a infraštruktúry informačných systémov, vrátane internetu, telekomunikačných sietí, počítačov, systémov a vstavaných procesorov a radičov"*.[21] V zákone o kybernetickej bezpečnosti je kybernetický priestor definovaný ako *„globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi"*.[22]

Kyberpriestor možno tiež opísať ako „*priestor zložený z troch komponentov: fyzická sieť, logická sieť a kybernetická osobnosť*".[23] Každý z týchto komponentov predstavuje odlišnú oblasť, v ktorej sa vykonávajú počítačové akcie.

Fyzická sieť je definovaná geografickým komponentom a komponentmi fyzickej siete. Geografická zložka sa týka polohy fyzických zložiek na súši, na mori, vo vzduchu alebo vo vesmíre. Napriek tomu, že geografické hranice medzi krajinami strácajú v kyberpriestore svoj význam, pretože rýchlosť svetla ich môže prekonať bez akejkoľvek kontroly, existujú prvky súvisiace s fyzickou sieťou ovplyvnenou suverenitou. Komponenty fyzickej siete pozostávajú z hardvéru, softvéru a prenosovej infraštruktúry (káble, bezdrôtové, satelitné alebo optické pripojenia), ktoré podporujú sieť, ako aj z potrebných fyzických konektorov (káble, smerovače, prepínače, servery, počítače). Logické konštrukcie sa používajú na podporu integrity a zabezpečenia v tomto prostredí. Fyzická zložka kyberpriestoru predstavuje hlavný cieľ pre

[19] BREZULA, J. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním – zborník príspevkov*. Bratislava : Akadémia policajného zboru, 2018, s. 143.

[20] *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020*, s. 24

[21] NIST. 2013. *Glossary of Key Information Security Terms*. Washington : United States Department of Commerce, 2013, s. 58

[22] *Zákon NR SR č. 69/2018 Z. z. o kybernetickej bezpečnosti*, § 3, písm. b)

[23] U.S. DoD. 2013. *Joint Publication 3-12. Cyberspace operations.* Washington : United States Department of Defense, 2013

SIGINT (Signal Intelligence[24]), MASSINT (Measurement and Signature Intelligence[25]), IMINT (Imagery Intelligence[26]), OSINT (Open-Source Intelligence[27]) a HUMINT (Human-Source Intelligence[28]).[29] Rovnakým spôsobom je primárna vrstva zvažovaná v analýze prostredníctvom GEOINT (Geospatial Intelligence[30]), ktorá môže prispieť k výberu cieľov v kyberpriestore.

Logická sieť pozostáva zo sieťových prvkov, ktoré sú prepojené abstraktnejšie ako vo fyzickej sieti. V tomto ohľade je príkladom databáza, ktorá je umiestnená na rôznych miestach, ale jej používatelia ju vnímajú ako jednu entitu.

Kybernetická osobnosť predstavuje vyššiu úroveň abstraktnosti v porovnaní s logickou sieťou. Pri vývoji digitálnej reprezentácie individuálnej identity používateľa alebo akejkoľvek entity v kyberpriestore sa riadi pravidlami logickej siete. Táto súčasť pozostáva z používateľov pripojených ku kyberpriestoru. Kybernetická identita môže súvisieť so skutočnou osobou, definovanou biografickými údajmi, e-mailovým účtom, IP adresou (internetový protokol), telefónnymi číslami alebo webovou adresou. Jedna osoba však môže vlastniť viacero kybernetických identít. Na druhej strane môže byť jedna kybernetická identita priradená ku viacerým skutočným používateľom. Dôsledkom týchto asociácií je, že priradenie zodpovednosti a výber cieľa sú v kyberpriestore náročné. Vzhľadom na to, že kybernetické identity môžu byť umiestnené na viacerých virtuálnych miestach, sú na vyhodnotenie situácie

[24] SIGINT (Signal Intelligence) je anglický výraz používaný špeciálnymi bezpečnostnými zložkami štátu ako sú rozviedka či kontrarozviedka a slúži na označenie informácií získaných pomocou týchto zdrojov: radarová prevádzka, dátová komunikácia, Internet, odpočúvanie telefónnych hovorov, snímanie vyžarovania monitora na diaľku a iné. Bližšie pozri: NSA / CSS. 2021. *Signals Intelligence*.

[25] MASSINT (Measurement and Signature Intelligence) - Meranie a podpisové spravodajstvo je technické odvetvie zhromažďovania spravodajských informácií, ktoré slúži na detekciu, sledovanie, identifikáciu alebo popis charakteristických vlastností pevných alebo dynamických cieľových zdrojov. Bližšie pozri: FAS. 2010. *Measurement and Signature Intelligence (MASINT)*.

[26] IMINT (Imagery intelligence) predstavuje spôsob zhromažďovania inteligencie, pri ktorej sa snímky analyzujú na identifikáciu informácií s inteligenčnou hodnotou. Bližšie pozri: SATCEN. 2021. *Introduction to Imaginery Intelligence (IMINT)*.

[27] OSINT (Open-Source Intelligence) - Spravodajstvo z otvorených zdrojov je typ informácií, ktoré využíva spravodajská služba a získaných z tzv. otvorených zdrojov, teda voľne dostupných informačných kanálov ako sú napr. denná tlač, internet, katastrálne knihy a pod. Nejedná sa teda o zdroje utajovaných informácií. Bližšie pozri: SANS. 2021. *Open-Source Intelligence (OSINT) Gathering and Analysis*.

[28] HUMINT (Human Intelligence) je jeden z druhov získavania informácií. Využívajú sa pri ňom schopnosti ľudských spolupracovníkov, ich tajné úlohovanie, riadenie a vyťažovanie, a to ako pre potreby špionáže, tak aj kontrašpionáže. HUMINT patrí k najúčinnejšiemu spôsobu zberu informácií, nakoľko môže odhaliť plány a zámery protivníka ešte vo fáze plánovania. Bližšie pozri: U.S. NWC. 2021. *Intelligence Studies: Human Intelligence (HUMINT)*.

[29] U.S. DoD. 2013. *Joint Publication 3-12. Cyberspace operations.* Washington : United States Department of Defense, 2013

[30] GEOINT (Geospatial Intelligence) predstavuje geopriestorové spravodajstvo o ľudskej činnosti na Zemi odvodené z využívania a analýzy snímok a geopriestorových informácií. Popisuje, hodnotí a vizuálne zobrazuje fyzické vlastnosti a geograficky súvisiace aktivity na Zemi. Bližšie pozri: OMNISCI. 2021. *GEOINT - Geospatial Intelligence*.

a dosiahnutie zamýšľaného účinku potrebné pokročilé možnosti zberu a analýzy spravodajských informácií.[31]

Pokiaľ ide o vzťahy s inými fyzickými doménami operačného prostredia, kybernetický priestor existuje v klasických dimenziách – pozemnej, námornej, vzdušnej a vesmírnej. Kyberpriestor je navyše definovaný agregáciou elektromagnetických zariadení umiestnených v uvedených štyroch fyzických doménach a prepojených káblami alebo bezdrôtovými pripojeniami s cieľom ukladať, spracovávať a vymieňať si informácie na podporu kognitívnej ľudskej dimenzie a na ovplyvnenie elektromechanických predmetov vo fyzickom priestore. Kyberpriestor teda nie je založený len na káblových prepojeniach na prenos údajov (doména CNO – Computer Network Operation[32]), ale aj na spojeniach založených na elektromagnetickom spektre (doména EW – Electronic Warfare[33]).

Hlavní aktéri v kyberpriestore

K hlavným aktérom, ktorí pôsobia v kyberpriestore patria:

a) Štátni aktéri, ktorí majú najvyšší potenciál vytvárať efekty v dôsledku prístupu k ľudským a materiálnym zdrojom. Dali by sa identifikovať medzi tradičnými protivníkmi, ale je možné aj zapojenie spojencov. Aby splnili stanovené ciele operácie v kyberpriestore je možné ich vykonávať priamo alebo prostredníctvom tretích strán.

b) Nadnárodné subjekty pozostávajú z oficiálnych a neoficiálnych organizácií, ktoré nie sú obmedzené geografickými hranicami medzinárodných hraníc. Tieto využívajú kyberpriestor na zhromažďovanie finančných zdrojov, na nábor, plánovanie a vykonávanie kybernetických útokov v tomto prostredí.

c) Kriminálne organizácie, ktoré kradnú informácie pre vlastné použitie alebo na účely ďalšieho obchodovania s nimi.

d) Malé skupiny alebo jednotliví aktéri, ktorí by mohli nelegálne pristupovať k počítačovým sieťam alebo jednotlivým systémom. V tomto prípade zámery pokrývajú širokú škálu, od identifikácie zraniteľností ako profesionálnej výzvy až po spôsobenie škody alebo šírenie sociálnych alebo politických správ, hoaxov, dezinformácií a pod.

e) Narušitelia – ide o zamestnancov, ktorí úmyselne alebo náhodne spôsobujú straty zamestnávateľom.[34]

---

[31] U.S. DoD. 2013. *Joint Publication 3-12. Cyberspace operations.* Washington : United States Department of Defense, 2013

[32] Bližšie pozri: NIST. 2021. *Computer Network Operation (CNO)*

[33] Bližšie pozri: ScienceDirect. 2021. *Electronic Warfare (EW)*

[34] U.S. DoD. 2013. *Joint Publication 3-12. Cyberspace operations.* Washington : United States Department of Defense, 2013

Charakteristiky a špecifiká kybernetických operácií

V kybernetickom priestore prebiehajú početné operácie aj v čase mieru, a to z mnohých dôvodov, napríklad kvôli identifikácii slabých stránok, zisteniu o zraniteľnosti protivníka, zhromažďovania spravodajských informácií alebo získavania konkurenčnej obchodnej výhody. Kybernetické operácie rovnako tak predstavujú prístupnejšie prostredie pre špionáž, podvratnú činnosť alebo sabotáž. Hlavné osobitosti kybernetických hrozieb sa týkajú prístupnosti vzdialených cieľov, asymetrického efektu, anonymity aktérov, časového aspektu a ich všestrannosti. Možnosť vykonávať akcie na diaľku umožňuje vykonávanie kybernetických operácií na lokálnej, regionálnej, ako aj globálnej úrovni vďaka nezávislosti kybernetických aktivít na administratívnych hraniciach. Výsledkom je, že je možné vykonávať kybernetické operácie, ktoré majú účinky vo fyzickom priestore, bez toho, aby do tohto priestoru zasahovali sily.[35]

Asymetrický efekt je výsledkom dostupnosti a možností realizovať aktivity v kyberpriestore pre všetky druhy organizácií, ako aj pre jednotlivcov. Malé organizácie, skupinky alebo dokonca jednotlivci, ktorí majú technickú kapacitu a potrebnú motiváciu, môžu vykonať útoky s rozsiahlymi účinkami, dokonca aj na strategickej úrovni. Typickým príkladom je kybernetický útok na Estónsko na jar 2007, keď hackeri na tri týždne výrazne obmedzili funkčnosť zariadení v telekomunikačných, bankových a ďalších doménach. Kybernetický útok mal ďalekosiahly finančný a sociálny dopad na estónsku spoločnosť.

Jedným z najvýznamnejších dôsledkov tohto útoku je skutočnosť, že kybernetické útoky boli zaradené do agendy NATO. Počas Varšavského samitu NATO v júli v roku 2016 bol kybernetický priestor vyhlásený za operačnú doménu vedľa tradičných domén: pozemnej, námornej, vzdušnej a vesmírnej. Okrem toho jedným z rozhodnutí ďalšieho samitu NATO, v Bruseli v júli v roku 2018, bolo zriadenie operačného centra pre kyberpriestor (Cyberspace Operation Center[36]) v Bruseli ako súčasti veliteľskej štruktúry NATO (NATO Command Structure).[37]

Časový aspekt operácií v kyberpriestore má pritom dve stránky. Na jednej strane môže byť čas potrebný na prípravu útokov veľmi krátky, najmä keď prístupová cesta, anonymita, vedľajšie účinky alebo zložitosť cieľa nie sú veľmi dôležité. Čas prípravy môže byť tiež dlhší, keď je potrebné vziať do úvahy uvedené faktory. Na druhej strane efekty v kyberpriestore môžu byť okamžité alebo úmyselne oneskorené. Táto funkcia ponúka vysokú flexibilitu na prispôsobenie jednotlivých aktivít celkovému tempu spoločných operácií. V prípadoch, keď je prístup k určitým cieľom ťažký, pretože ho nemožno zaručiť v pravý čas, je možné rozhodnúť sa pre oneskorený účinok.

---

[35] U.K. MoD. 2016. *Cyber Primer*. London : United Kingdom Ministry of Defence, Development, Concepts and Doctrine Centre, 2016

[36] Bližšie pozri: NATO. 2021. *Cyber Defence*.

[37] NATO. 2018. *Brussels Summit Declaration*.

Ďalšou charakteristikou aktivít v kyberpriestore je anonymita. Keďže tieto činnosti je napriek technologickému pokroku ťažké sledovať a lokalizovať, väčšinu kybernetických útokov je možné odmietnuť. Nerozpoznané útoky s neidentifikovanými autormi tak znižujú politické riziko a perspektívu možnej odvety. Možná reakcia je z pohľadu obetí kybernetických útokov náročná kvôli neistote pri identifikácii autorov útokov.

Kybernetické útoky sa zároveň vyznačujú univerzálnosťou, pretože ich vplyv môže byť reverzibilný alebo upravený tak, aby bol stupeň ich vplyvu na služby variabilný, podľa výberu útočníka. Kybernetický útok, ktorý preruší napájanie priemyselného zariadenia, môže byť napríklad zastavený a napájanie obnovené. Táto črta môže znížiť vedľajšie škody a spôsobiť, že kybernetické útoky by mohli byť nejakým spôsobom akceptované zo sociálneho a politického hľadiska.

Využitie kybernetických schopností v nadnárodných operáciách sa líši od spolupráce vo fyzickom prostredí. Ak sa vo fyzickom prostredí operačné plánovanie zaoberá väčšinou fyzickými spôsobilosťami jednotiek pozemných, vzdušných, námorných alebo špeciálnych síl, v kybernetickom priestore sa integrácia zameriava viac na účinky národných príspevkov než na samotné spôsobilosti.[38]

Vplyv operácií v kyberpriestore

Kyberpriestor sa vďaka dynamickému rozvoju IKT v ostatných rokoch rozvinul do takej miery, že v ňom prebieha, resp. na ňom závisí značný počet aktivít v politickej, ekonomickej, sociálnej, energetickej, bezpečnostnej alebo vojenskej oblasti, čím sa stáva vysoko zraniteľným v dôsledku narušenia jeho fungovania alebo zničenia. Dôležitosť kybernetických operácií stále rastie kvôli významu kybernetického priestoru pre systémy riadenia a velenia a závislosti od nechránených sietí, akými sú napríklad verejný internet.

Na rozdiel od fyzických oblastí sa v kyberpriestore môžu vlastné aj nepriateľské sily pohybovať rýchlosťou pohybujúcou sa od rýchlosti zvuku po rýchlosť svetla, čo sťažuje sledovanie a hodnotenie situácie. Kybernetická sila sa môže pohybovať z jednej strany zemegule na druhú stranu v priebehu pár milisekúnd, pričom pokrýva všetky operačné úrovne, od taktických, cez operačné, až po strategické. Aj keď sú geografické oddelenia pre kyberpriestor možné, v závislosti od pozemných, vzdušných alebo priestorových obmedzení alebo spojení v uzle, táto charakteristika spôsobuje problémy s rozdelením úrovne velenia (taktické, operačné, strategické). Prepojenie kyberpriestoru s fyzickými doménami tiež spôsobuje problémy s velením a riadením kybernetických síl hlavnými zložkami síl (pozemnými, námornými a vzdušnými).

Vplyv realizovaných akcií v kyberpriestore a účinky na vojenské operácie sú spojené s velením a riadením na všetkých úrovniach rozhodovania. Velenie a riadenie na operačnej

[38] DUCARU, S. 2018. *NATO advances in its new operational domain: Cyberspace*.

úrovni je hlavným nástrojom veliteľov pre organizáciu a synchronizáciu činností pre rôzne kategórie síl s cieľom splniť stanovené strategické ciele. Systém velenia a riadenia (C2 – Command and Control) však nemôže byť účinný bez dobre vyvinutého systému C4 (Command, Control, Communication, Computers = velenie, riadenie, komunikácia, počítače), ktorý pokrýva celú operačnú oblasť. V dnešnej dobe už bez takéhoto systému nie je možné velenie a riadenie síl pre plánovanie a vykonávanie operácií.

Systémy velenia a riadenia sú založené na komunikačných a počítačových systémoch, softvéri a ďalších službách prepojených nielen káblami, ale aj bezdrôtovými pripojeniami na prenos údajov. Pretože tieto systémy sú prepojené s inými globálnymi informačnými systémami, možno konštatovať, že sú súčasťou kyberpriestoru. V dôsledku toho môžu udalosti, ktoré sa vyskytnú v kyberpriestore, pozitívne alebo negatívne ovplyvniť systémy velenia a riadenia, ktoré ovplyvnia systému velenia a riadenia vykonávanú veliteľom na podriadených silách.

Okrem systému C2 závisia na efektívnom systéme C4 aj ďalšie prevádzkové funkcie, ako sú napríklad spravodajstvo alebo logistika. Napríklad v americkej doktríne spravodajských informácií o spoločných operáciách[39] sa zdôrazňuje dôležitosť toho, že architektúra zdieľajúca spravodajské produkty by mala používať globálnu informačnú mriežku. Opatrenia, ktoré sa odohrávajú v kyberpriestore totiž výrazným spôsobom ovplyvňujú celý spravodajský proces. Podobne musia rôzne systémy spolupracovať kvôli koordinácii realizovaných akcií[40], čo zvyšuje zraniteľnosť voči rôznym udalostiam v kyberpriestore.

Prevádzková ochrana znamená integráciu viacerých komponentov na zaistenie efektívnej a účinnej ochrany vojenských i nevojenských zdrojov energie. Tieto komponenty zahŕňajú spravodajské informácie, ochranu informačných systémov, rakety a ďalšie kľúčové zariadenia. Všetky závisia od toho, či systémy C2 fungujú jednotlivo alebo spoločne, a sú ovplyvnené operáciami v kyberpriestore. Ďalšou operačnou funkciou, ktorá potrebuje automatizáciu a ktorá závisí od jednotlivých prvkov v rámci informačných technológií, je logistická podpora. Automatizované logistické a ďalšie informačné systémy môžu byť taktiež ovplyvnené udalosťami v kyberpriestore.

Možno povedať, že velenie a riadenie, spravodajské služby, logistická podpora a ďalšie prvky a služby sú závislé od prístupu do kyberpriestoru a od činností, ktoré sa tam uskutočňujú. Ak sa teda berie do úvahy údržba, prevádzka a ochrana tej časti kyberpriestoru, ktorá podporuje prepojenie rôznych systémov, existuje riziko zmeny jednej alebo viacerých operačných funkcií, čo má za následok ohrozenie splnenia vytýčených operačných a strategických cieľov.

Ďalším efektom závislosti operačných funkcií na kyberpriestore je analýza z pohľadu protivníka. Kyberpriestor totiž poskytuje spôsob, ako ovplyvniť jednu alebo viac operačných

[39] U.S. DoD. 2013. *Joint Publication 2-0. Joint Intelligence.* Washington : United States Department of Defense, 2013

[40] ELLIOT, M. C. *Operational Command and Control of Joint Task Force Cyberspace Operations.* Newport, Naval War College, USA : Research Report, 2008

funkcií protivníka, na ktorého možno v jeho jadre útočiť priamo alebo nepriamo. Preto je potrebné analyzovať protivníkove schopnosti pôsobenia v kyberpriestore a zvážiť vlastné schopnosti pôsobenia proti nemu, aby sa maximalizovala šanca naplniť vlastné operačné i strategické ciele.

Záver

Na záver je možné skonštatovať niekoľko základných faktov. Dimenzie súčasného bojiska sa skladajú z fyzickej a kybernetickej zložky. Žiadnu z dimenzií nemožno považovať za izolovanú, pretože aktivita v jednej dimenzii môže mať zásadné dôsledky na ostatné dimenzie a aktivity v nich prebiehajúce. Z tohto dôvodu je dôležité určiť spôsob vzájomnej interakcie rôznych komponentov bojového priestoru, aby sa zaistila účinná správa bojiska.

Informačná doba vytvára nové zásady vedenia operácií na základe prepojenia medzi jednotlivými aktérmi a vybavením (zariadeniami, zbraňami, zbraňovými systémami, technikou, výstrojom, výzbrojou atď.) používaným na bojisku. Kľúčovým prvkom na vytvorenie výhody oproti súperovi je dosiahnutie informačnej prevahy. Z hľadiska informačného manažmentu je nevyhnutné, aby sa správne informácie mohli prenášať správnej osobe v správnom čase a v použiteľnom formáte, aby sa uľahčilo situačné povedomie a rozhodovanie.

Fyzická zložka kyberpriestoru je hlavným cieľom pre analýzy SIGINT, MASSINT, OSINT a HUMINT a hlavnou vrstvou pre analýzy GEOINT. Viaceré spravodajské disciplíny preto musia brať do úvahy rôzne aspekty kyberpriestoru. Operácie v kyberpriestore sú plánované a vykonávané dokonca aj v čase mieru na lokálnej alebo globálnej úrovni, pričom fyzická prítomnosť v cieľovom priestore nie je potrebná.

Možnosť vytvárať efekty rýchlosťou svetla spôsobuje ťažkosti pri vytváraní veliteľskej úrovne pre kybernetické operácie (taktické, operačné, strategické) a pri vytváraní prvkov velenia a riadenia pre hlavné zložky síl (pozemné, námorné, vzdušné). Ak vezmeme do úvahy tendenciu prepájať vojenskú komunikáciu s globálnou, akcie v kybernetickom priestore majú vplyv na väčšinu operačných funkcií (velenie a riadenie, spravodajské služby, streľbu, logistickú podporu, operačnú ochranu a pod.).

Zoznam použitej literatúry a zdrojov:

ALBERTS, D. S. – GARSTKA, J. J. – STEIN, F. P. 2010. *Network Centric Warfare: Developing and Leveraging Information Superiority*. [online] [cit. 26-02-2022] Dostupné na: <http://www.dodccrp.org/files/Alberts_NCW.pdf>

ANDRASSY, V. – GREGA, M. – NEČAS, P. 2018. *Crisis Management and Simulations*. Ostrowiec Swietokrzyski : Wyzsza Szkola Biznesu i Przedsiebiorczości w Osrtowcu Swietokrzyskim, 2018. 202 s. ISBN 978-83-64557-33-0.

ANDRASSY, V. – GREGA, M. 2015. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2. s. 11-18. ISSN 1338-4880.

BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním – zborník príspevkov*. Bratislava: Akadémia policajného zboru, 2018. ISBN 978-80-8054-773-8.

ELLIOT, M. C. *Operational Command and Control of Joint Task Force Cyberspace Operations.* Newport, Naval War College, USA : Research Report, 2008. [online] [cit. 28-02-2022] Dostupné na: <http://www.dtic.mil/dtic/tr/fulltext/u2/a484515.pdf>

FABIÁN, M. – MINTÁL, J. M. – UŠIAK, J. 2020. EU Security Threats Resulting from Disinformation in Cyberspace. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, s. 116-139. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

FAS. 2010. *Measurement and Signature Intelligence (MASINT)*. [online] [cit. 27-02-2022] Dostupné na: <https://fas.org/irp/program/masint.htm>

GREGA, M. – ŽENTEK, M. – NEČAS, P. 2020. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, s. 172-229. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

HROMADA, M. 2017. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133. ISBN 978-80-87500-89-7.

KAZANSKÝ, R. 2020. The Conflict in Cyberspace – Definitions Frame. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in the Cyberspace*, 2020, s. 32-68. Krakov : University of Public and Individual Security „Apeiron" in Krakow. ISBN 978-83-64035-70-8.

KOLLÁR, D. 2020. Current Trends and Challenges in the Cyberspace and Cyber Security. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, p. 10-31. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Fakulta medzinárodných vzťahov Ekonomickej univerzity. Bratislava : Vydavateľstvo Ekonóm, 2018, ISBN 978-80-225-4506-8.

KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti 2020 – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87. ISBN 978-80-8054-879-7.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LUKÁŠ, L. a kol.: *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017. 220 s. ISBN 978-80-87500-89-7.

NATO. 2018. *Brussels Summit Declaration*. [online] [cit. 25-02-2022] Dostupné na: <https://www.nato.int/cps/en/natohq/official_texts_156624.htm>

NATO. 2018. NATO Calls On Taliban To Join Ceasefire. In *ForcesNet*, 2018. [online] [cit. 26-02-2022] Dostupné na: <https://www.forces.net/news/nato-calls-taliban-join-ceasefire>

NATO. 2021. *Cyber Defence*. [online] [cit. 28-02-2022] Dostupné na: <https://www.nato.int/cps/en/natohq/topics_78170.htm>

NIST. 2021. *Computer Network Operation (CNO)*. [online] [cit. 27-02-2022] Dostupné na: <https://csrc.nist.gov/glossary/term/computer_network_operations>

NSA / CSS. 2021. *Signals Intelligence*. [online] [cit. 27-02-2022] Dostupné na: <https://www.nsa.gov/what-we-do/signals-intelligence/>

OMNISCI. 2021. *GEOINT – Geospatial Intelligence*. [online] [cit. 27-02-2022] Dostupné na: <https://www.omnisci.com/technical-glossary/geoint>

RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 161-173. ISBN 978-80-8054-773-8.

SANS. 2021. *Open-Source Intelligence (OSINT) Gathering and Analysis*. [online] [cit. 27-02-2022] Dostupné na: <https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/>

SATCEN. 2021. *Introduction to Imaginery Intelligence (IMINT)*. [online] [cit. 27-02-2022] Dostupné na: <https://www.satcen.europa.eu/page/introduction_to_imagery_intelligence_imint_>

ScienceDirect. 2021. *Electronic Warfare (EW)*. [online] [cit. 28-02-2022] Dostupné na: <https://www.sciencedirect.com/topics/engineering/electronic-warfare>

SIGHOLM, J. 2016. Non-State Actors in Cyberspace Operations. In *Journal of Military Studies*, 2016, roč. 4, č. 1, s. 1-37. ISSN 1799-3350. [online] [cit. 25-02-2022] Dostupné na: <https://ccdcoe.org/research/tallinn-manual/>

SINGER, P. W. – FRIEDMAN, A. 2014. *Cybersecurity and Cyberwar (What Everyone Needs to Know)*. Oxford : Oxford University Press, 2014. 306 s. ISBN 978-0-19991-811-9.

SMEETS, M. 2017. Organizational integration of offensive cyber capabilities: A primer on the benefits and risks. In *9th International Conference on Cyber Conflict (CyCon) – Conference Proceedings*. Tallinn : IEEE, 2017. ISSN 2325-5374.

U.K. MoD. 2016. Cyber Primer. Development, concepts and doctrine centre, 2016. [online] [cit. 27-02-2022] Dostupné na: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf>

U.S. DoD. 2010. *Joint Publication 1-02. Dictionary of Military and Associated Terms*. United States of America, Department of Defense, 2010

U.S. DoD. 2013. *Joint Publication 2-0. Joint Intelligence.* United States of America, Department of Defense, 2013

U.S. DoD. 2013. *Joint Publication 3-12. Cyberspace operations.* United States of America, Department of Defense, 2013

U.S. DoD. 2014. *Joint Publication 3-13. Information Operations*. United States of America, Department of Defense, 2014

U.S. NWC. 2021. *Intelligence Studies: Human Intelligence (HUMINT)*. [online] [cit. 26-02-2022] Dostupné na: <https://usnwc.libguides.com/c.php?g=494120&p=3381553>

VALUCH, J. 2019. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava : Wolters Kluwer, 2019. 160 s. ISBN 978-80-571-0154-3.

Van HAASTER, J. 2019. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019. 359 s. [online] [cit. 25-02-2022] Dostupné na: <https://pure.uva.nl/ws/files/37093787/Thesis.pdf>