ÚTOČNÉ KYBERNETICKÉ OPERÁCIE AKO SÚČASŤ HYBRIDNÝCH HROZIEB

OFFENSIVE CYBER OPERATIONS AS PART OF HYBRID THREATS

plk. gšt. v. z. 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:

Physical reality is connected to cyber reality, any action in cyberspace ultimately produces a kinetic effect. States have understood this relationship and while the United States hegemony of physical military strength is without doubt, intense fights are carried out for reaching the leading position in cyberspace thinking that by winning the cyberwar means winning on both realms. In order to cause as much damage as possible, in the context created by the information era in which we find ourselves, state or non-state actors, considered hybrid threats, choose to operate in cyberspace mainly through offensive cyber operations. Offensive cyber operations are unconventional asymmetric operations that allow a hybrid threat to operate anonymously, to use forces belonging to proxy actors, to avoid symbolic triggers while producing devastating kinetic effects, without time and space limitations, combined with other unconventional operations such as psychological operations, information operations, or electronic warfare.

Keywords: offensive cyber operations, hybrid threat, cyber space.

Abstrakt:

Fyzická realita je prepojená s kybernetickou realitou a tak každá činnosť v kybernetickom priestore vytvára v konečnom dôsledku kinetický efekt. Štáty tento vzťah pochopili a napriek tomu, že o hegemónii americkej vojenskej fyzickej sily niet pochybností, v súčasnosti sa vedú intenzívne boje o dosiahnutie vedúceho postavenia v kyberpriestore v domnienke, že víťazstvo v kybernetickej vojne znamená víťazstvo v oboch sférach. Preto sa, v kontexte vytvorenom informačnou érou, v ktorej sa nachádzame, štátni alebo mimovládni aktéri snažia spôsobiť svojim protivníkom čo najväčšie škody v kyberpriestore predovšetkým prostredníctvom útočných kybernetických operácií. Útočné kybernetické operácie sú nekonvenčné asymetrické operácie, ktoré umožňujú v rámci hybridnej hrozby pôsobiť anonymne, využívať sily patriace zástupcom aktérov, vyhýbať sa symbolickým spúšťačom a vytvárať devastačné kinetické efekty bez časového a priestorového obmedzenia v kombinácii s inými nekonvenčnými operáciami, ako sú psychologické operácie, informačné operácie alebo elektronický boj.

Kľúčové slová: útočné kybernetické operácie, hybridná hrozba, kybernetický priestor.

Úvod

Aktéri, pôsobiaci a vyvíjajúci aktivity v oblasti bezpečnosti a obrany, sa v súčasnosti snažia prostredníctvom hybridných hrozieb získať, udržať, prípadne posilniť svoj vplyv v tretích krajinách, najmä prostredníctvom aktivít zameraných na občiansku spoločnosť. Podľa telekomunikačných expertov na konci roku 2018 používalo internet približne 51,2 % svetovej populácie, t. j. cca 3,9 miliardy ľudí.[1] Dnes, v druhej polovici roku 2021, vzhľadom na dynamický vývoj ľudskej spoločnosti v oblasti informačných a komunikačných technológií, je tento počet už oveľa vyšší, pričom do konca roku 2023 by podľa odhadov Medzinárodnej telekomunikačnej únie mal dosiahnuť až 70 %, t. j. 5,3 miliardy ľudí.[2] Pri takomto obrovskom počte užívateľov môžu útočné kybernetické operácie úspešné a zabezpečiť splnenie vytýčených cieľov, pretože prinášajú mnoho príležitostí a výhod pre tých, ktorí sú schopní ich realizovať, resp. plánujú ich realizovať.

Napriek tomu, že pri vedení útočných kybernetických operácií sa využíva aj civilná infraštruktúra, odborníci, ktorí pôsobia v tejto oblasti, odporúčajú začlenenie útočných kybernetických spôsobilostí do vojenského systému,[3] pretože operácie v kybernetickom priestore môžu umožniť slobodu konania a realizáciu aktivít v iných oblastiach.[4]

Aj preto je primárnym cieľom autora článku, využijúc relevantné metódy vedeckého výskumu, nadväzujúc na práce renomovaných zahraničných i domácich autorov z oblasti bezpečnosti a zvlášť zo sféry kybernetickej bezpečnosti (Smeetsa[5], Stevensa[6], Van Haastera[7], Sigholma[8], Singera a Friedmana[9], Hromadu[10], Lukáša[11], Korauša[12], Gregu[13], Fabiána[14],

---

[1] ITU. *Global Cybersecurity Index (GCI) 2018*. Geneva : International Telecommunication Union, 2019, s. 6
[2] Tamtiež
[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, s. 3
[4] U.S. DoA. The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, s. 8
[5] 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
[6] STEVENS, T. Cyberweapons: an emerging global governance architecture. In *Palgrave Communications*, 2017, roč. 3, č. 1
[7] Van HAASTER, J. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019
[8] SIGHOLM, J. Non-State Actors in Cyberspace Operations. In Journal of Military Studies, 2016, roč. 4, č. 1
[9] SINGER, P. W. – FRIEDMAN, A. Cybersecurity and Cyberwar (What Everyone Needs to Know®). Oxford : Oxford University Press, 2014.
[10] HROMADA, M. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I*. Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133.
[11] LUKÁŠ, L. a kol. *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017.
[12] 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
[13] 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
[14] 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

Kazanského[15], Kollára[16], Valucha[17], Andrassyho[18] a ďalších) a vychádzajúc zo syntézy definičných aspektov útočných kybernetických operácií, čiže z definície konceptu, štruktúry a ich účinkov a tiež toho, ako niektoré štáty kladú dôraz na rozvoj kybernetických spôsobilostí, rozšíriť percepciu kybernetickej bezpečnosti a poukázať prostredníctvom tohto vedeckého výskumu na vojenský potenciál útočných kybernetických operácií v rámci hybridných hrozieb.

1. Útočné kybernetické operácie

Predmetom výskumu sú útočné kybernetické operácie (ďalej len „OCO" = Offensive Cyber Operations), t. j. kybernetické operácie vedené vojenskými alebo polovojenskými silami, pod velením a/alebo pod kontrolou štátov alebo neštátnych aktérov, zamerané na využitie slabých stránok protivníka, jeho zraniteľností, implementáciu rôznych techník narušania kyberpriestoru, schopnosť preťažiť ťažko dostupné kybernetické ciele a presadzovanie cielených škodlivých kybernetických produktov[19], ktoré pôsobia na nepriateľské sily. V americkej vojenskej doktríne sú OCO definované ako „*operácie v kybernetickom priestore navrhnuté tak, aby premietali silu prostredníctvom použitia síl v kyberpriestore alebo prostredníctvom neho*".[20]

Z koncepčného hľadiska sa OCO a kybernetické útoky rozlišujú podľa spôsobu organizácie, veľkosti účinkov a dôvodov, ktoré stoja za nimi. OCO predstavujú starostlivo naplánované kybernetické útoky (môžu byť priamo integrované do operačného plánu), ktoré sa prostredníctvom značných škôd spôsobených vybraným cieľom zameriavajú na získanie výhod pre štáty alebo pre určité skupiny v prípade neštátnych útočníkov. Na rozlíšenie týchto dvoch konceptov môžu poslúžiť dva nasledujúce príklady. Kým vypustenie vírusu Stuxnet (objaveného v júni 2010) bolo OCO, pretože zničilo nevyhnutné zariadenie (odstredivky) v iránskych zariadeniach na obohacovanie uránu v Natanz[21] pozastavením ich postupu pri získavaní jadrovej zbrane (čo bolo v záujme iných štátov), ransomware WannaCryptor (WannaCry) z roku 2017 bol „iba" kybernetický útok, ktorý spustili hackeri, ktorí šifrovali informácie na infikovaných počítačoch, aby získali nejaké osobné odmeny za ich dešifrovanie

---

[15] 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.

[16] 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

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

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

[19] 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, s. 6

[20] U.S. DoA. *FM 3-12 Cyberspace and Electonic Warfare Operations*, s. 18

[21] KELLEY, M. B. The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. In *Insider*, 2013

(čo bolo „len“ v záujme daných hackerov). Nepotvrdili sa pri ňom obvinenia Severnej Kórey zo strany USA a Spojeného kráľovstva.[22]

Pokiaľ ide o štruktúru OCO, má klasickú formu kybernetického útoku a postupne zahŕňa nasledovné kroky:

- prieskum, t. j. získavanie údajov o dátovej prevádzke cieľa, úrovni kybernetickej bezpečnosti a možných účtoch, ktoré môžu byť odcudzené;
- vniknutie, ktoré môže byť na užívateľskej úrovni alebo s administrátorskými právami počítačového systému;
- získanie oprávnení využitím zraniteľností operačného systému alebo softvérového balíka;
- dosiahnutie cieľa, inštalácia zadných vrátok, počítačová špionáž, poškodzovanie alebo pozmeňovanie súborov a pod.[23]

Výsledkom OCO môže byť odmietnutie (zrušenie kontroly nad zdrojmi držanými nepriateľom), degradácia (zníženie operačnej kapacity nepriateľa), narušenie (úplné, alebo dočasné zablokovanie nepriateľa), zničenie (trvalé, úplné a nenapraviteľné odmietnutie prístupu alebo činnosť cieľa) alebo manipulácia (kontrola alebo výmena informácií, počítačových systémov a/alebo nepriateľských sietí spôsobom, ktorý podporuje jeho vlastné ciele).[24]

V roku 2020 vedci z Belferovho Centra pre vedu a medzinárodné záležitosti na Harvardskej univerzite v USA vypracovali rebríček najmocnejších štátov sveta podľa ich kybernetickej sily (1. Spojené štáty, 2. Čína, 3. Spojené kráľovstvo, 4. Rusko, 5. Holandsko, 6. Francúzsko, 7. Nemecko, 8. Kanada, 9. Japonsko, 10. Austrália).[25] Zároveň vypracovali aj ďalšie poradie, a to najútočnejších štátov v kyberpriestore. Z tohto rebríčka je vidieť, že najútočnejším štátom na svete sú Spojené štáty nasledované Spojeným kráľovstvom. Na ďalších miestach sú: 3. Rusko, 4. Čína, 5. Španielsko, 6. Izrael, 7. Nemecko, 8. Irán, 9. Holandsko a 10. Francúzsko.[26]

2. Príležitosti, ktoré ponúkajú OCO v rámci hybridných hrozieb

Hybridné útočné akcie, ktorých súčasťou sú OCO, ponúkajú viac príležitostí na zapojenie síl. V nasledujúcom texte sú uvedené príklady hlavných výhod získaných prostredníctvom OCO v rámci hybridných hrozieb, ktoré sa prejavujú v kyberpriestore.

---

[22] BBC. Cyber-attack: US and UK blame North Korea for WannaCry. In *BBC News*, 2017>

[23] 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, s. 6

[24] Van HAASTER, J. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019, s. 195

[25] SUSSMAN, B. Top 10 Most Powerful Countries in Cyberspace. In *SecureWorld*, 2021

[26] Tamtiež

2.1 Kybernetické zbrane

Kybernetická zbraň je zdrojový kód, ktorý sa používa alebo je navrhnutý tak, aby slúžil na účely ohrozenia alebo spôsobenia fyzického, funkčného alebo duševného poškodenia štruktúr, systémov, ľudí alebo iných živých tvorov[27], pričom môže mať mnoho foriem: vírusy (samoreplikačné programy, ktorých šírenie si vyžaduje činnosť človeka), červy (podtrieda vírusov, ktoré sa môžu šíriť bez ľudského zásahu), trójske kone (škodlivý softvér skrytý v legitímnom programe), útoky za účelom odmietnutia služby (bombardovanie serverov správami, ktoré môžu spôsobiť ich zlyhanie) a phishing (falošné e-maily a webové stránky) ktoré ľudí oklamú, aby odhalili informácie o svojom hesle).[28]

Pokiaľ ide o hybridné hrozby, používanie kybernetických zbraní môže ponúknuť alternatívy, ktoré iné prostriedky alebo metódy vojny neposkytujú, najmä preto, že nie sú fyzickými nástrojmi a nemožno ich ľahko odhaliť, zmerať alebo zakázať obchodovanie s nimi. Kybernetické zbrane sú prístupné akejkoľvek hybridnej hrozbe. Dajú sa kúpiť na Dark Web (zbierka webových stránok, na ktoré je prístup iba prostredníctvom určitých vyhľadávacích nástrojov), pričom ceny sa pohybujú od 1 USD.[29] Vďaka flexibilite a vysokému stupňu voľnosti v spôsobe ich prevádzky sú kybernetické zbrane veľmi účinné a využívané v rámci hybridných hrozieb.

2.2 Ochrana síl

Hybridné hrozby realizované prostredníctvom OCO môže ovplyvniť spôsob, akým aktér zameriava alebo koncentruje svoju silu, a to tak, že znemožní protivníkovi detekovať jeho útoky, napríklad zrušením alebo falošným spustením niektorých senzorov. Rovnako tak aj narušením schopností reagovať na OCO, čo nevyhnutne prispieva k posilneniu ochrany vlastných síl.[30]

Typickým príkladom ochrany síl vykonávanej s pomocou OCO počas vojenskej operácie je akcia, pri ktorej v roku 2007 Izrael zničil údajný sýrsky jadrový reaktor v provincii Deir al-Zour.[31] Izrael, zapojením OCO na operačnej úrovni, uskutočnil úspešnú leteckú operáciu bez strát spôsobených sýrskou protivzdušnou obranou.[32]

Operácia Ruska v Gruzínsku v roku 2008 je zasa príkladom synchronizácie OCO s konvenčnými operáciami, vďaka čomu bol dosiahnutý vyšší stupeň ochrany ruských vojenských jednotiek. Webové stránky gruzínskych úradov a médií v Gori boli napadnuté

---

[27] STEVENS, T. Cyberweapons: an emerging global governance architecture. In *Palgrave Communications*, 2017, roč. 3, č. 1, s. 2
[28] NIC. *Global trends 2030: Alternative Worlds*. National Intelligence Council, 2012, s. 85
[29] GOMEZ, M. Dark Web Price Index 2020. In *Privacy Affairs*, 2021
[30] CILLUFFO, F. J. – CLARK, J. R. Thinking Through Cyber's Role in Ground Combat. In Military Review, 2015, č. 1, s. 3-4
[31] BBC. Israel admits striking suspected Syrian nuclear reactor in 2007. In *BBC News*, 2018
[32] CILLUFFO, F. J. – CLARK, J. R. Thinking Through Cyber's Role in Ground Combat. In Military Review, 2015, č. 1, s. 2

kybernetickými útokmi typu DDoS predtým, ako ruské lietadlá vstúpili do vzdušného priestoru Gruzínska,[33] takže ruské jednotky získali cenný čas, počas ktorého mohli obsadiť strategické pozície bez nejakej väčšej reakcie zo strany protivníkových síl.

V rovnakom zmysle možno v kontexte vyššie uvedených informácií doplniť, že „kybernetickí bojovníci" majú vysoký stupeň ochrany pred možnými odvetami svojich cieľov, pretože môžu operovať zo vzdialených a chránených oblastí.

2.3 Anonymita agresora

Vzhľadom na povahu kyberpriestoru útočníci môžu často skrývať pôvod svojich útokov alebo ich môžu viesť tak, že ich útoky voči druhej strane vyzerajú, akoby ich viedol niekto iný, tretia strana. Príkladom útoku „pod falošnou vlajkou" je útok z roku 2014, keď bola Severná Kórea (prostredníctvom organizácie bojujúcej proti počítačovej kriminalite známej ako Dark Seoul) obvinená z organizovania rozsiahleho OCO proti spoločnosti Sony Pictures, čo sa však nepotvrdilo, pretože útoky proti Sony boli vedené z viacerých stredísk po celom svete, vrátane Kongresového centra v Singapure a Univerzity Thammasat v Thajsku.[34]

Možnosť spustenia OCO z iných štátov umožňuje vyhnúť sa akýmkoľvek odvetným opatreniam, pretože to môže viesť k nechcenému konfliktu. Aj keď môže byť zdroj OCO lokalizovaný, je ťažké dokázať, že agresor konal na príkaz štátnych orgánov, najmä preto, že štáty z útokov vinia zločinecké organizácie alebo obvinenia úplne popierajú.[35]

2.4 Ničivé kinetické efekty

Je ťažké predpovedať rozsah strát, ktoré môžu byť spôsobené útočnou kybernetickou operáciou. Ničivé účinky môžu siahať od ľudských strát (napr. v dôsledku zastavenia dodávky elektriny do nemocníc alebo do jadrových elektrární) až po veľké finančné straty a materiálne škody (napr. v dôsledku zničenia serverov alebo počítačov v systéme banky/burzy, rozbitia podnikových účtov alebo zverejnenia obchodného tajomstva).

Minulé udalosti predstavujú určite silné argumenty na podporu tejto schopnosti. Najrelevantnejší príklad, ktorý je možné ponúknuť, sa stal v auguste 2012, deň pred veľkým islamským náboženským sviatkom, keď vírus, neskôr nazývaný Shamoon, zničil pevné disky 30 000 počítačov patriacich saudskoarabskej národnej ropnej spoločnosti Saudi Aramco, ktorá patrí medzi najdôležitejšie prvky saudskej kritickej infraštruktúry. Vírus vymazal pamäť infikovaných počítačov a vložil do nich obrázky horiacej americkej vlajky.[36] História oplýva

---

[33] HOLLIS, D. Cyberwar Case Study: Georgia 2008. In *Small Wars Journal*, 2011, s. 5
[34] SANGER, D. E. – PERLROTH, N. U.S. Said to Find North Korea Ordered Cyberattack on Sony. In *The New York Times*, 2014
[35] ANDRES, R. Cyber Gray Space Deterrence. In *The Journal of Complex Operations*, 2017, roč. 7, č. 2, s. 94
[36] IASIELLO, E. Are Cyber Weapons Effective Military Tools?" In *Military and Strategic Affairs*, 2015, roč. 7, č. 1, s. 30

viacerými podobnými príkladmi, ktoré sa zdajú byť útočnými kybernetickými operáciami, nielen izolovanými kybernetickými útokmi, ktoré priniesli značné straty.

2.5 Homogenita s inými nekonvenčnými operáciami

Sila hybridnej hrozby je daná najmä nekonvenčnými operáciami, ktoré spúšťa. Tieto musia byť synchronizované a využívané v kombinácii s inými operáciami a inovatívnym spôsobom. Nekonvenčné prvky hybridnej hrozby predstavujú homogénny celok, v ktorom sa komplementárnosť prvkov tiež stáva multiplikátorom sily pre konvenčné prvky.

Napriek tomu, že OCO sú využívané v informačnom prostredí, nie sú to informačné operácie, a možno ich ľahko použiť v kombinácii so všetkými ostatnými operáciami špecifickými pre informačné prostredie: informačné operácie, psychologické operácie a elektronický boj.

Vo vzťahu k iným nekonvenčným operáciám môže hybridná hrozba využívať OCO tromi spôsobmi:

a) Na podporu ďalších nekonvenčných operácií. Na taktickej úrovni môžu OCO vykonávať tímy integrované do taktických jednotiek síl v špeciálnych operáciách. Napríklad mikroštruktúra špeciálnych operácií, ktorá zahŕňa aj špecialistu OCO, môže preniknúť do protivníkovej vojenskej štruktúry a prostredníctvom OCO môže získať prístup do dátovej siete, z ktorej bude môcť začať informačné operácie.
b) Podporované inými nekonvenčnými operáciami. OCO môže byť podporované informačnými operáciami, najmä operáciami s využitím sociálnych médií a sietí v kyberpriestore. Tento argument je podporený tým, že umožňujú ľahký zber údajov a metadát. Metadáta získané prostredníctvom operácií s využitím sociálnych sietí v kyberpriestore sú dôležité pre úspech OCO, pretože môžu poskytnúť údaje o dobe, v ktorej je cieľ aktívny, sociálnu skupinu cieľa, konkrétne aplikácie, ktoré cieľ používa, typ zariadenia, z ktorého sa pripája a dokonca aj hardvérovú a softvérovú konfiguráciu.
c) Súbežne s inými nekonvenčnými operáciami. Aktér sa prostredníctvom hybridných hrozieb snaží vyvolať u civilného obyvateľstva cieľového štátu strach (obavy) rôznymi psychologickými operáciami, súčasne môže dosiahnuť rovnaký výsledok tým, že sa OCO využijú ako kybernetický terorizmus, pričom sa poškodia prvky kritickej infraštruktúry, ako napríklad zrušenie kontroly nad priehradou, čo môže spôsobiť ničivé záplavy.[37]

2.6 Bez časových a priestorových obmedzení

Využívanie kyberpriestoru na hybridné hrozby znamená slobodu konať mimo fyzických a časových prekážok, ktoré spôsobuje geografický priestor, geopolitický kontext a/alebo časové

[37] HERRICK, D. The social side of 'cyber power'? Social media and cyber operations. In *9th International Conference on Cyber Conflict (CyCon)*. Tallinn : IEEE, 2017, s. 108.

požiadavky na operácie. Táto príležitosť je celkom očividná a rovnako cenná. S OCO je možné pripraviť bojisko dlho predtým, ako začnú nepriateľské akcie, pričom sa to nijako nedotýka zásady strategického prekvapenia, rýchlej akcie a synchronizácie s inými plánovanými formami útoku. Kybernetická zbraň zavedená do kyberpriestoru, v ktorom nepriateľ operuje, môže byť spustená v najvhodnejšom čase pre plánované operácie. Prevádzka v kyberpriestore nevyžaduje žiadne logistické náklady, ako sú náklady na dopravu vojakov a materiálu. OCO nie sú ani časovo tak náročné ako ostatné konvenčné vojenské akcie.

2.7 Nejednoznačnosť právneho režimu

Aj keď existuje niekoľko ustanovení týkajúcich sa právneho inštitútu sankcionovania počítačových útokov, napríklad Dohovor Rady Európy o počítačovej kriminalite[38] a Tallinská príručka[39], produkt Centra výnimočnosti NATO pre spoluprácu v oblasti kybernetickej obrany (CCDCOE) zaoberajúca sa OCO z hľadiska ius in bello, požadované efekty sa zatiaľ nedosiahli. Jednou z prekážok sankcionovania OCO je fakt, že nie je možné určiť, kedy je OCO použitím sily národného štátu alebo iba trestnou činnosťou individuálneho aktéra, prípadne zločineckej skupiny, pretože je ťažké určiť prepojenie medzi útočníkom (skutočnou osobou vykonávajúcou útok) a národným štátom kontrolujúcim operáciu.

Prísne predpisy týkajúce OCO navyše vyžadujú medzinárodný konsenzus (vrátane nečlenských krajín NATO alebo EÚ), ktorý nie je možné dosiahnuť, pretože aj veľká väčšina z nich (Spojené štáty a Spojené kráľovstvo sú dve najútočnejšie krajiny sveta v kyberpriestore) využíva tieto nekonvenčné operácie na hybridné akcie.

Doteraz nedošlo k žiadnemu ozbrojenému zásahu proti hybridnej hrozbe, ktorá využíva OCO, pretože existujúca právna nejednoznačnosť ponecháva akúkoľvek možnú ozbrojenú reakciu bez právnej validácie. V tejto súvislosti je potrebné poznamenať, že sa tak nestalo ani v roku 2007, keď Estónsko žiadalo NATO, aby vyhlásilo, že bola porušená jeho suverenita, čo by spôsobilo uplatnenie článku 5 Washingtonskej zmluvy o kolektívnej sebaobrane.[40]

Hybridné hrozby prostredníctvom OCO pripravujú tým najúčinnejším spôsobom kyberpriestor na boj, v čase keď je ešte mier, bez obáv z odvetných zásahov zo strany ich cieľov.

2.8 Využívanie síl patriacich tretím stranám

Táto výhoda sa prejavuje v možnosti štátu, v ktorom sa nachádza počítačový agresor, najať si na vykonanie operácie kybernetických žoldnierov alebo prilákať „bezplatných kybernetických bojovníkov“. V rámci hybridných hrozieb tak dochádza k využívaniu značného počtu polovojenských aktérov a/alebo niekedy dokonca zločineckých organizácií. Aby sa

[38] FUNTA, R. 2021. *Dohovor Rady Európy o počítačovej kriminalite*. Bratislava : Wolters Kluwer, 2021.
[39] CCDCOE. 2017. *Tallinn Manual*
[40] SINGER, P. W. – FRIEDMAN, A. *Cybersecurity and Cyberwar (What Everyone Needs to Know®)*. Oxford : Oxford University Press, 2014

zmenili nekonvenčné metódy podľa požiadaviek boja, hybridná hrozba potrebuje rýchlo obnoviteľné sily, ktoré je možné počas operácií ľahko odstrániť. Tieto potreby pokrývajú sily patriace tretím stranám.

Sigholm sa vo svojej práci pokúsil identifikovať najdôležitejších neštátnych aktérov, ktorí môžu byť dočasne aktívni v kyberpriestore, a zároveň analyzoval dôvody útokov, cieľov a metód. Medzi tých, ktorí môžu realizovať alebo participovať na OCO patria najmä:

- prvotriedni kybernetickí útočníci, autori škodlivého obsahu a hackeri (hacktivisti, hackeri „black hat“, vlastenecký hackeri alebo členovia organizácií zaoberajúcich sa počítačovou kriminalitou), ktorí sú veľmi skúsení a sú schopní spôsobiť veľké škody;
- Niche kybernetickí útočníci, kybernetickí votrelci a počítačoví podvodníci;
- kybernetickí vojaci, amatérski hackeri a zombie počítače (zahrnuté v botnete, ktorý spúšťa útoky DDoS); táto skupina je veľmi užitočná, pretože je najpočetnejšia, je tiež najľahšie ovládateľná a môže efektívne podporovať OCO bez vysokej spotreby zdrojov.[41]

2.9 Účinnosť voči technologicky vyspelým štátom

Technologicky vyspelé štáty sa do značnej miery spoliehajú na kybernetický priestor z dôvodov spojených s riadením veľkej populácie. Obyvateľstvo týchto štátov je sústredené v hustých mestských oblastiach (megapolách) s miliónmi obyvateľov, ktorými sú spravidla hospodárske a administratívne centrá. Tieto husto obývané mestské aglomerácie pracujú s obrovskými množinami údajov a prepojenými senzormi, zariadeniami a softvérovými systémami. Tieto aspekty spoločne vytvárajú veľkú zraniteľnosť technologicky vyspelých štátov.

Prepojenie používaných systémov (dohľad, poplach, kontrola cestnej infraštruktúry a pod.) v kyberpriestore vytvára riziko, že hybridná hrozba prostredníctvom OCO môže využiť najslabší systém z hľadiska kybernetickej bezpečnosti a preniknúť a spôsobiť poškodenie alebo narušenie reťazca v celej systémovej sieti. Potenciálne krízy, ktoré môžu vzniknúť, môžu byť ešte vážnejšie, pretože husté mestské oblasti sú spravidla aj centrami moci, ktorých napadnutie spôsobí problémy pre stabilitu a bezpečnosť technologicky vyspelých štátov.

2.10 Vyhýbanie sa symbolickým spúšťačom

Za zmienku stojí určite aj fakt, že prostredníctvom OCO sa dá vyhnúť tzv. symbolickým spúšťačom[42], ako ich vo svojom článku nazýva Andres. Ich výhoda v tomto kontexte spočíva v tom, že nevyvolávajú také silné emocionálne reakcie občianskej spoločnosti ako fyzické útoky, ktorá zväčša následne slepo podporuje odvetné (mnohokrát aj iracionálne) akty násilia.

---

[41] SIGHOLM, J. Non-State Actors in Cyberspace Operations. In *Journal of Military Studies*, 2016, roč. 4, č. 1, s. 11-12

[42] ANDRES, R. Cyber Gray Space Deterrence. In *The Journal of Complex Operations*, 2017, roč. 7, č. 2, s. 5

Možno ak by japonská armáda namiesto útoku na Pearl Harbour v roku 1941 alebo al-Káida namiesto útoku na dvojičky v roku 2001 (čo pritiahlo pozornosť a veľmi silno pobúrilo drvivú väčšinu amerického obyvateľstva) zvolili OCO na dosiahnutie svojich cieľov, politická reprezentácia krajiny by nezískala takú veľkú podporu pre neskoršie vojenské úsilie USA a legislatívne opatrenia prijímané v rámci boja s terorizmom.

Silné emócie v občianskej spoločnosti totiž nevyvolajú technické detaily o ničivých účinkoch OCO, ale citlivé zábery zničených, zdemolovaných budov alebo trpiacich, zranených osôb (symbolické spúšťače). Navyše, informácie o OCO, ktoré sú, resp. boli vedené proti národu (štátu), nemajú vysoký stupeň transparentnosti z dôvodov týkajúcich sa úrovne utajenia informácií. Nikto výslovne nechce, aby veľa ľudí vedelo, aká je zraniteľnosť používaných systémov, štátu, aké kybernetické zbrane boli použité, a pod. Úspešnosť útočných operácií spustených hybridnou hrozbou je spojená aj s úrovňou pasivity alebo podpory, ktorú má medzi populáciou cieľového štátu a OCO túto rovnicu negatívne neovplyvňuje.

Záver

Na záver je možné v súvislosti s vyššie uvedenými informáciami uviesť, že bez ohľadu na to, či sa informačná prevaha získava prostredníctvom OCO, alebo sa protivníkovi „len“ odopiera prístup k informáciám, získané výsledky majú rovnakú váhu pri dosahovaní víťazstva. Viaceré štáty (najmä USA, Spojené kráľovstvo, Holandsko, Nemecko, Francúzsko, Rusko, Čína, Izrael, Irán a ďalšie), ale aj neštátne subjekty, rozvíjajúce hybridnú taktiku, sa v ostatnej dobe v čoraz väčšej miere zamerali na operacionalizáciu OCO, nakoľko pochopili ich výhody a uvedomujú si príležitosti, ktoré je možné týmto spôsobom dosiahnuť. Je im tiež zrejmé, že OCO môžu mať zásadný, rozhodujúci vplyv na ich úspech v hybridnej vojne.

Pre každého aktéra, či už štátneho alebo neštátneho, je potrebné dôkladne porozumieť prostriedkom, ktoré protivník využíva, a aj podľa toho určiť ďalší konkrétny postup zameraný na dosiahnutie víťazstva nad ním alebo na elimináciu jeho spôsobilostí. To bez akýchkoľvek pochybností platí aj v kybernetickom priestore.

Možnosti, ktoré OCO ponúka hybridnému agresorovi, sú veľmi rozmanité. Nie sú obmedzené geografickým priestorom a časom, umožňujú anonymnú prevádzku, medzinárodný zákaz je neúčinný, nie sú tzv. symbolickými spúšťačmi a dajú sa vykonávať v kombinácii s nekonvenčnými operáciami. Je síce otázne, do akej miery sa tí, ktorí vykonávajú hybridné operácie, budú orientovať na útočné kybernetické operácie, nech je však odpoveď akákoľvek, zvyšovanie úrovne kybernetickej bezpečnosti na národnej i medzinárodnej úrovni je dnes mimoriadne dôležité v záujme zaistenia celkovej bezpečnosti spoločnosti (štátu, aliancie) a vyhnutiu sa prekvapeniam a nepríjemnostiam, ktoré s OCO súvisia.

Zoznam použitej literatúry a zdrojov:

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.

ANDRES, R. 2017. Cyber Gray Space Deterrence. In *PRISM, the journal of complex operations*, 2017, roč. 7, č. 2, s. 91-98. ISSN 2157-0663. [online] [cit. 18-08-2021] Dostupné na: <https://cco.ndu.edu/PRISM-7-2/Article/1401927/cyber-gray-space-deterrence/>

BARIČIČOVÁ, Ľ. 2018. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 8-15. ISBN 978-80-8054-773-8.

BBC. 2017. Cyber-attack: US and UK blame North Korea for WannaCry. In *BBC News*, 2017. [online] [cit. 18-08-2021] Dostupné na: <https://www.bbc.com/news/world-us-canada-42407488>

BBC. 2018. Israel admits striking suspected Syrian nuclear reactor in 2007. In *BBC News*, 2018. [online] [cit. 18-08-2021] Dostupné na: <https://www.bbc.com/news/world-middle-east-43481803>

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.

CCDCOE. 2017. *Tallinn Manual*. [online] [cit. 19-08-2021] Dostupné na: <https://ccdcoe.org/research/tallinn-manual/>

CILLUFFO, F. J. – CLARK, J. R. 2015. Thinking Through Cyber's Role in Ground Combat. In *Military Review*, 2015, č. 1, s. 1-4. ISSN 5684-2127. [online] [cit. 19-08-2021] Dostupné na: <http://cchs.auburn.edu/_files/shoot-move-communicate.pdf>

DIXON, R. 2016. Bringing big data to war in megacities. In *Military Intelligence Professional Bulletin*, 2016, roč. 42, č. 3. s. 61-66. ISSN 2379-2167. [online] [cit. 19-08-2021] Dostupné na: <https://www.armyupress.army.mil/Portals/7/Primer-on-Urban-Operation/Documents/Military-Intelligence-Professional-Bulletin-July-to-September-2016.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.

FUNTA, R. 2021. *Dohovor Rady Európy o počítačovej kriminalite*. Bratislava : Wolters Kluwer, 2021. 140 s. ISBN 978-80-571-0365-3.

GOMEZ, M. 2021. Dark Web Price Index 2020. In *Privacy Affairs*, 2021. [online] [cit. 19-08-2021] Dostupné na: <https://info.publicintelligence.net/GlobalTrends2030.pdf>

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.

HERRICK, D. 2017. The social side of 'cyber power'? Social media and cyber operations. In *9th International Conference on Cyber Conflict (CyCon)*. Tallinn : IEEE, 2017. ISSN 2325-5374. [online] [cit. 18-08-2021] Dostupné na: <https://ieeexplore.ieee.org/document/7529429>

HOLLIS, D. 2011. Cyberwar Case Study: Georgia 2008. In *Small Wars Journal*, 2011. [online] [cit. 18-08-2021] Dostupné na: <https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>

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.

IASIELLO, E. 2015. Are Cyber Weapons Effective Military Tools?" In *Military and Strategic Affairs*, 2015, roč. 7, č. 1, s. 23-40. ISSN 2307-8634. [online] [cit. 18-08-2021] Dostupné na: <https://www.inss.org.il/wp-content/uploads/systemfiles/2_Iasiello.pdf>

ITU. 2019. *Global Cybersecurity Index (GCI) 2018*. Geneva : International Telecommunication Union, 2019. 92 s. ISBN 978-92-61-28201-1. [online] [cit. 18-08-2018] Dostupné na: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>

KAZANSKÝ, R. 2020. Conflict in cyberspace - framework of definitions. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, s. 32-68. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

KELLEY, M. B. 2013.The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. In *Insider*, 2013. [online] [cit. 18-08-2021] Dostupné na: <https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>

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.

KORAUŠ, A. – VESELOVSKÁ, S. – KELEMEN, P. 2017. Cyber security as part of the business environment. In *Aktuálne otázky svetovej ekonomiky a politiky – zborník z konferencie Medzinárodné vzťahy 2017:*. Bratislava : Vydavateľstvo Ekonóm, 2017. 1113 s. ISBN 978-80-225-4488-7.

KOSTRECOVÁ, E. - JÓKAY, M. - KOSTREC, M. 2010. *Počítačová kriminalita*. Bratislava: Slovenská technická univerzita, 2010. 109 s. ISBN 978-80-227-3410-3.

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

MAJCHÚT, I. 2018. Súčasné bezpečnostné aspekty. In *Národná a medzinárodná bezpečnosť 2018 – zborník vedeckých a odborných prác z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. ISBN 978-80-8040-568-7.

NIC. 2012. *Global trends 2030: Alternative Worlds*. National Intelligence Council, 2012. 160 s. ISBN 978-1-929667-21-5. [online] [cit. 19-08-2021] Dostupné na: <https://www.privacy affairs.com/dark-web-price-index-2020/>

SANGER, D. E. – PERLROTH, N. 2014. U.S. Said to Find North Korea Ordered Cyberattack on Sony. In *The New York Times*, 2014. [online] [cit. 18-08-2021] Dostupné na: <https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html>

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. 19-08-2021] 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.

STEVENS, T. 2017. Cyberweapons: an emerging global governance architecture. In *Palgrave Communications*, 2017, roč. 3, č. 1. ISSN 2055-1045. [online] [cit. 19-08-2021] Dostupné na: <https://www.nature.com/articles/palcomms2016102>

SUSSMAN, B. 2021. Top 10 Most Powerful Countries in Cyberspace. In *SecureWorld*, 2021. [online] [cit. 19-08-2021] Dostupné na: <https://www.secureworld.io/industry-news/top-10-most-powerful-countries-in-cyberspace>

U.S. Department of the Army. 2010. *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*. [online] [cit. 18-08-2018] Dostupné na: <https://fas.org/irp/doddir/army/pam525-7-8.pdf>

U.S. Department of the Army. 2017. *FM 3-12 Cyberspace and Electonic Warfare Operations*. [online] [cit. 18-08-2021] Dostupné na: <https://fas.org/irp/doddir/army/fm3-12.pdf>

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. 18-08-2021] Dostupné na: <https://pure.uva.nl/ws/files/37093787/Thesis.pdf>