DOI: https://doi.org/10.52651/nmb.c.2023.9788080406516.142-150

14. medzinárodná vedecká konferencia ♦14th International Scientific Conference
Národná a medzinárodná bezpečnosť 2023 ♦ National and International Security 2023
19. – 20. 10. 2023, Liptovský Mikuláš

KYBERNETICKÉ OPERÁCIE AKO SÚČASŤ KYBERNETICKÝCH HROZIEB

CYBER OPERATIONS AS THE PART OF CYBER THREATS

Vojtech JURČÁK, Vladimír ANDRASSY, Katarína STOLÁRIKOVÁ

ABSTRACT

This article was supported by the Research and Development Support Agency based on Contract No. APVV-20-0334.

Today's world is becoming more vulnerable, more dangerous. The development of the security environment is becoming more dynamic and difficult to predict. The concept of security, defined by Barry Buzan and his scientific team in the 80s of the last millennium, extends to the field of cyber security. We are increasingly encountering cyber-attacks, which represent a global security threat to the world. Cyber space is becoming another dimension where military operations can take place on land, sea, in the air and in space. Cyber space was defined by the NATO summit in Wales, September 2014 and later at the Warsaw NATO summit, July 2016 in the form of the Alliance's commitment in the field of cyber defence. The NATO confirms to follow the principle of restraint and to support the maintenance of international peace, security and stability in cyberspace. In the article, the authors point out some manifestations of cyber-attacks, the need to protect cyber and information systems and in a close historical excursion, they analyse the effects of these attacks in stages of their development.

Keywords: Cyber Security, Cyber-attack, Cyber Space, Cyber warfare

ÚVOD

Ešte nedávno existovala iba jedna realita - hmotný svet. Všetko sa zmenilo s príchodom internetu. Virtuálna realita digitálneho sveta začala dokonca meniť hmotný svet a udalosti. Rozvoj informačných a komunikačných technológií priniesol s masovým využívaním internetu veľa pozitívneho, na druhej strane však i nové hrozby pre jednotlivcov, spoločenské skupiny, národy, štáty, svet – stal sa globálnou bezpečnostnou hrozbou.

Téma informačnej a kybernetickej bezpečnosti rezonuje u odbornej i laickej verejnosti už niekoľko rokov, no v roku 2016 nabrala vďaka celospoločenským udalostiam na vážnosti a stala sa jednou z hlavných tém médií, ale aj verejných diskusií. Závislosť jednotlivcov, spoločností a štátov od informačných technológií sa stáva čoraz silnejšou, merateľnejšou a masívnejšou. V súčasnej dobe sa už fyzická realita stáva akýmsi doplnkom virtuálnej reality. Hlavnú úlohu v našich životoch hrá „kyber-fyzicky systém". Ukazuje sa, že globálne informačné siete sú istým druhom mozgu a nervového systému pre svet, v ktorom sa fyzicky nachádzame (Rubanov 2017). Za významné v roku 2016 (Summit NATO vo Varšave) sa považuje i zaradenie kybernetického priestoru do ďalšej dimenzie, v ktorej predpokladá NATO vykonávať svoje operácie.

Na prelome rokov 2016 a 2017 bola kybernetická bezpečnosť diskutovaná najmä v súvislosti s prezidentskými voľbami v USA, keď americké úrady opakovane obvinili Ruskú federáciu z neoprávneného vniknutia do korešpondencie vedenia a členov ústredia kampane

Demokratickej strany Hillary Clintonovej s cieľom diskreditácie jej osoby. Ruská vláda poprela akúkoľvek spojitosť s ruskou kyberšpionážnou skupinou Fancy Bear, ktorá údajne za útokom stála. Rovnako stála aj za vniknutím do serverov Svetovej antidopingovej agentúry, keď zverejnili lekárske záznamy popredných športovcov, poukazujúc na užívanie podporných medicínskych prostriedkov ako odpoveď na škandál za pozitívne dopingové testy ruských športovcov na letnej a zimnej olympiáde a paraolympiáde.

Je nepopierateľným faktom, že viaceré svetové veľmoci využívajú informačné technológie k dosahovaniu svojich strategických cieľov - politických, ekonomických, spoločenských či vojenských. Nie je žiadnym tajomstvom, že najúčinnejší spôsob získavania informácií spočíva vo využití technologických prostriedkov. Informačné technológie sa teda dajú využívať okrem kybernetických útokov na strategické ciele aj na kybernetickú špionáž. Kyberneticky priestor ako sústava hmotných a virtuálnych prvkov má kriticky dopad na hmotný svet vrátane jeho pozemného, námorného, vzdušného a kozmického priestoru. Vo svojej komplexnosti vplýva na všetkých aktérov a všetky prvky operačného prostredia. Pokiaľ ide o kybernetickú obranu, strategická koncepcia NATO zdôrazňuje potrebu rozvíjať schopnosť predchádzať, odhaľovať, brániť a zotavovať sa z útokov v kybernetickom priestore. Frekvencia a sofistikovanosť týchto hrozieb sa rapídne zvyšuje, preto hrozby vychádzajúce z kybernetického priestoru predstavujú pre Alianciu značnú výzvu. NATO v oblasti obrany kybernetického priestoru:

- integruje aspekty obrany kybernetického priestoru do štruktúr a procesov plánovania operácií NATO;
- zameriava sa na prevenciu, odolnosť a obranu kritických súčastí kybernetického priestoru;
- rozvíja obranyschopnosť v oblasti kybernetického priestoru a centralizuje ochranu vlastných sietí NATO;
- poskytuje pomoc spojencom s cieľom dosiahnuť minimálnu úroveň obrany kybernetického priestoru a znížiť zraniteľnosť kritickej infraštruktúry;
- spolupracuje s partnermi, medzinárodnými organizáciami, súkromným sektorom a akademickou obcou (AJP-01, 2017).

Kľúčovým prvkom národnej obrany je vojenská koncepcia C4ISR (velenie, riadenie, komunikácia, počítače, spravodajstvo, dohľad a prieskum). Model C4ISR sa zakladá na velení a riadení (Command & Control), ktoré spravujú pozemné, námorné a vzdušné sily, využívajúc spravodajské informácie z informačných, monitorovacích a prieskumných platforiem. Zároveň sú tieto prvky závislé na komunikácii a samozrejme, ako sa zväčšila veľkosť a zložitosť vojenských operácií, tak sa zvýšila aj ich závislosť od počítačov (STO-MP-MSG-143).

Estónsky minister zahraničných vecí Urmas Paet uviedol, že „kyberútoky sú virtuálne, psychologické a skutočné.” (Davis 2007).

Mnohí obhajcovia informačnej vojny tvrdia, že kybernetická sabotáž je oveľa humánnejší spôsob vedenia vojny než bombové a raketové útoky. Je to preto, že elektronické útoky nepredstavujú okamžité fyzické nebezpečenstvo pre civilistov tak, ako výbušniny. Znepokojujúca je ale skutočnosť, že útoky na počítačovú infraštruktúru krajiny vážne destabilizujú jej hospodárstvo a sprostredkovane pôsobia na spoločnosť.

Ene Ergma, estónska politička a vedkyňa, roky skúmala jadrovú energiu a sledovala, ako sa svet transformuje príchodom jadrovej technológie. Informačná vojna je pre ňu podobným definujúcim momentom vo svetových dejinách: „Keď sa pozriem na jadrový výbuch a výbuch, ktorý sa v našej krajine uskutočnil v máji 2007, vidím to isté. Rovnako ako

jadrová radiácia, ani kybernetická vojna nespôsobí krvácanie, ale môže zničiť všetko." (Davis 2007).

Generálny riaditeľ Agentúry NATO pre komunikácie a informácie, Koen Gijsbers, uviedol, že: „Kybernetická hrozba, ktorú vnímame, je veľmi reálna a veľmi vážna. Sofistikované útoky na siete, ktoré sú základom našej spoločnosti, sa môžu vykonávať odkiaľkoľvek na svete. Kybernetická hrozba sa stáva globálnou hrozbou. Najúčinnejšia obrana pre vlády a súkromný sektor je vzájomná spolupráca krajín, založená na informovanosti (zdieľaní informácii o kybernetických útokoch, dobrej praxe pri možnostiach ochrany a pod.) a dôvere. Silné kybernetické partnerstvo priemyslu NATO je kľúčom k boju proti hrozbám, ktorým čelíme a k zvýšeniu našej kolektívnej odolnosti a bezpečnosti". (STO-MP-MSG-143)

Všetky krajiny deklarujú obrannú úlohu kybervojsk. Ministerstvo obrany USA po vytvorení kybervojenského veliteľstva vyhlásilo, že hoci má US Cyber Command celý rad útočných schopností, zakladá sa na obrannej stratégii. Aj napriek skutočnosti, že väčšina kybervojsk disponuje útočnými prostriedkami, žiadna krajina neuznáva útoky na informačné systémy iných krajín. Avšak došlo aj k takýmto útokom. (Rubanov 2017)

Globálne informačné siete sú nervovým systémom hmotného sveta. Škody, ktoré spôsobia hrozby vyplývajúce z „kybernetických zbraní" a nepriateľských aktivít v kybernetickom priestore možno porovnávať so zbraňami hromadného ničenia. Z toho dôvodu by sa mali aj kybervojská riadiť tým, čo je deklarované v oficiálnych dokumentoch. Ich zámerom má byť ochrana v boji proti počítačovej kriminalite. Špeciálne metódy získavania informácií kybervojskom v službách spravodajstva sú takisto súčasťou opatrení na ochranu svojich národných záujmov. (Rubanov 2017)

1 KYBERNETICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ INFORMÁCIÍ

Bezpečnosť môžeme definovať ako istotu, kedy na životne dôležité hodnoty referenčného objektu deštruktívne nepôsobia žiadne entity, subjekty, procesy a to ako v rámci referenčného objektu, tak i v jeho okolí (Jurčák a kol., 2020). Z tejto všeobecnej definície bezpečnosti môžeme vychádzať aj pri definovaní kybernetickej bezpečnosti (ďalej len „KB"). Ak uvažujeme, že svetové spoločenstvo považuje dáta (informácie) za dôležitú hodnotu, musí prijímať opatrenia na ochranu ich spravovania, prenosu a ukladania. Referenčným objektom v tomto prípade je každý kybernetický systém a jeho zosieťovanie, hodnotou sú dáta. Na základe uvedeného potom môžeme definovať ***kybernetickú bezpečnosť*** *ako istotu, kedy dáta kybernetického systému nie sú vystavené vonkajším, prípadne vnútorným hrozbám pri ich vytvorení, prenose, ukladaní a využívaní, prípadne odstránení* (vlastná konštrukcia). Za bezpečnostnú hrozbu môžeme považovať akúkoľvek udalosť, ktorá môže poškodiť kybernetický systém a jeho aktíva.

Objektami ochrany (referenčnými objektmi), v rámci informačných systémov a informačných a komunikačných technológií môžu byť napríklad obsahy súborov alebo serverov, pravosť hlasov vo voľbách, dostupnosť procesov elektronického obchodu, či prístup k utajovaným informáciám a zariadeniam, ale aj zariadenia kritickej infraštruktúry, prípadne už uvedené vojenské komunikačné zariadenia (Ivančík 2020). Tieto informácie sú ukladané, spracovávané a prenášané na základe požiadaviek ich majiteľov, akými sú napríklad prísna kontrola ich dostupnosti, modifikácie a šírenia. Cieľom sú teda opatrenia na ochranu informácií (majetku) pred rozličnými hrozbami hackerov, iných používateľov, počítačových procesov či rôznych nehôd, ktoré môžu dané informácie znehodnotiť z hľadiska dostupnosti,

integrity a dôvernosti. Tieto opatrenia sa vzťahujú na cieľ hodnotenia a na operačné prostredie, v ktorom daný produkt informačnej a komunikačnej technológie pôsobí.

Ján Hochmann, ktorý sa ako expert Národného bezpečnostného úradu podieľal na príprave legislatívy o kybernetickej bezpečnosti, definuje digitálny priestor a kyberneticky priestor. ***Digitálny priestor*** *tvoria informačné a komunikačné technológie a procesy v rámci nich, ale aj informácie a údaje, vzťahy medzi nimi a tiež podpornú infraštruktúru*. ***Kyberneticky priestor*** *definuje ako časť digitálneho priestoru, ktorý pozostáva zo všetkých informačných systémov prepojených na globálnej dátovej úrovni, ktorých základom je internet, pričom prvky v izolovanom priestore nie sú jeho súčasťou* (Hochmann, 2016).

Slovenská republika z hľadiska ukotvenia kybernetickej ochrany svojich občanov výrazne zaostáva. Práve preto ľudia vnímajú kybernetickú ochranu len z médií a rôznych firemných školení a neuvedomujú si skutočné dopady kybernetických incidentov, čo následne viedlo k zmapovaniu rôznych druhov malvérov a k výskumu ich charakteristík a dopadov na spoločnosť.

2 KYBERNETICKÁ VOJNA

Kybernetická vojna je pojem, ktorý nie je jednoznačne definovaný. Podľa Jirásek, Novák, Požár, 2013 predstavuje tento pojem *použitie počítačov a internetu na vedenie vojny v kybernetickom priestore a predstavuje súbor rozsiahlych, často politicky či strategicky motivovaných, súvisiacich a vzájomne vyvolaných organizovaných kybernetických útokov a protiútokov.*

Vo všeobecnosti je pojem vojna definovaný Carl von Clausewitzom ako akt násilia s cieľom donútiť protivníka, aby sa podriadil našej vôli (Clausewitz, 1996, s. 23), alebo vojna ako pokračovanie politiky inými prostriedkami (Clausewitz, 1996, s. 36). Prídavné meno k pojmu vojna označuje, o aký druh vojny sa jedná, alebo aké prostriedky na jej vedenie boli použité. V našom prípade sa jedná o kybernetické prostriedky a teda kybernetickú vojnu. Na základe uvedeného môžeme napísať, že ***kybernetická vojna*** *je akt násilia s cieľom donútiť protivníka, aby sa podriadil našej vôli, pričom násilie odpovedá kybernetickému násiliu (útoku) v kybernetickom priestore,* alebo *pokračovanie politiky s použitím kybernetických prostriedkov v kybernetickom priestore* (vlastná konštrukcia).

2.1 POČIATKY KYBERNETICKEJ VOJNY

Vírus Creeper, ktorý bol začiatkom 70-tych rokov detegovaný vo vojenskej počítačovej sieti USA „ARPANET" (predchodca moderného internetu), je jedným z prvých dôkazov zraniteľnosti akýchkoľvek systémov a zariadení pripojených na sieť.

Mnohí autori publikujúci na internetových portáloch hovoria o „Prvej svetovej kybernetickej vojne". Vyskytuje sa aj vyraz „Web War One" a niektorí ju datujú od roku 2007, keď hackeri ochromili desiatky vládnych a firemných stránok v Estónsku. Počiatky „Prvej svetovej kybernetickej vojny" sa však objavili už začiatkom 90-tych rokov.

Americká armáda demonštrovala revolučný vojensky potenciál informačných technológií už počas vojny v Perzskom zálive v rokoch 1990 až 1991. S leteckými útokmi a technickými prostriedkami americké jednotky zničili komunikačnú infraštruktúru velenia a riadenia (command and control) Saddáma Husajna ešte predtým, než sa zamerali na ich tankové a ďalšie bojové jednotky. V začiatkoch operácie „Púštna búrka" proti Iraku za inváziu do Kuvajtu USA nasadili vírusy do irackých vojenských počítačových systémov. Po vojne v Perzskom zálive až do polovice 90-tych rokov USA využívali hackerské nástroje

najmä na boj proti drogovým kartelom prenikaním do ich bankových účtov a marením finančných transakcií. (Frontline, 2016)

V rokoch 1990 a 1991 prenikli hackeri z Holandska do počítačových systémov Ministerstva obrany USA. Vyhľadávali informácie o jadrových zbraniach, riadených strelách, „Púštnom štíte" a „Púštnej búrke". V decembri 1994 prenikli neznámi hackeri do počítačových systémov Americkej námornej akadémie. V rokoch 1995 a 1996 útočník z Argentíny prenikol do univerzitného systému USA, odkiaľ sa dostal do počítačových sietí v Laboratóriu námorného výskumu, NASA a ďalších inštitúcií rezortu obrany. Získal citlivé výskumné informácie, ako napríklad o dizajne lietadiel, radarovej technológii a satelitnom inžinierstve. V máji 1996 identifikoval Hlavný účtovný úrad USA, že počítačové útoky na systémy Ministerstva obrany predstavujú rastúce riziká. Podľa údajov Agentúry pre ochranu informačných systémov (DISA) rezort obrany USA mohol už v roku 1995 čeliť až 250 000 útokom, pričom ich počet sa každoročne zdvojnásobuje vďaka masívnemu nárastu používania internetu a zvyšujúcej sa sofistikovanosti hackerov a ich nástrojov. Ochrana pred týmito útokmi stojí značné finančné prostriedky, no v najhoršom prípade sú vážnou hrozbou pre národnú bezpečnosť, pretože útočníci ovládli celé obranné systémy, z ktorých mnohé podporujú kritické funkcie ako je výskum a vývoj zbrojných systémov, logistika a financie. (Frontline, 1996)

2.2 KYBERNETICKÝ ÚTOK V JUHOSLÁVII

Americky vojensky novinár Robert Parry v apríli 1999 citoval spravodajské zdroje, ktoré tvrdili, že keď začali bombové útoky NATO (24. marca 1999), americké sily na Balkáne boli zle pripravené na rozsiahlejšiu „informačnú vojnu". Navyše v rámci NATO bolo vtedy ťažké nájsť konsenzus o takýchto nových taktikách. (Frontline, 2016)

Neznámi srbskí počítačoví hackeri začiatkom apríla 1999 zablokovali a na niekoľko dní znefunkčnili hlavný webový server ústredia NATO v Bruseli, ktorý informoval verejnosť o operácii NATO v Kosove pod vedením USA a obsahoval aj prepisy brífingov a hodnotení škôd bombových útokov. Zároveň zablokovali emailový server NATO dvomi tisíckami správ denne. John Pike, obranný a spravodajsky analytik, na margo tohto útoku povedal, že ide o učebnicový príklad nízko nákladného útoku s vysokou hodnotou. (Frontline, 1996) Následne NATO schválilo rozšírené operácie, americká armáda zmobilizovala expertné tímy a začala prekvapovať rôznymi technologickými trikmi. Prvá široko používaná aplikácia technologického vojenstva bola „mäkká bomba", ktorá sa vyskytla 2. mája 1999, keď vybuchla nad juhoslovanskou elektrárňou, vypustila uhlíkové vlákna nad elektrickými vedeniami a zapríčinila skraty, ktoré na sedem hodín odpojili veľkú časť Juhoslávie od elektrickej energie. „Máme určité zbrane, o ktorých nehovoríme," povedal generálmajor Charles Wesley Clark, najvyšší veliteľ NATO počas bombového útoku NATO proti Juhoslávii. (Frontline, 2016)

Spočiatku sa táto „info-vojna" sústredila iba na bojisko. V ranných fázach konfliktu v Juhoslávii sústredilo NATO svoje útoky na centrá velenia a riadenia. USA a NATO sofistikovanými elektronickými útokmi na počítače srbskej protivzdušnej obrany napadli siete systémov PVO a systémov riadenia letovej prevádzky vtedajšej Juhoslávie. Pentagon vtedy deklaroval svoj úspech pri likvidácii srbskej protivzdušnej obrany rušením a poškodzovaním údajov v srbských počítačoch prostredníctvom mikrovlnných prenosov. V takejto elektronickej ofenzíve proti Srbsku bola už vtedy americká spravodajská služba schopná zájsť oveľa ďalej za hranice klasického vojenského hackerstva (vrátane spôsobovania výpadkov elektrickej energie). Americkí „info-bojovníci" už boli schopní vysielať vírusy do civilných počítačových systémov, meniť bankové záznamy, vypnúť telefónny systém a vo všeobecnosti

tak narúšať infraštruktúru vtedajšej Juhoslávie, ako aj získať prístup k vládnym bankovým účtom používaným pri nákupe vojenských dodávok alebo k osobným účtom juhoslovanských lídrov. Krajiny ako napríklad vtedajšia Juhoslávia s nie veľmi vyspelými a slabo zabezpečenými počítačmi, ktoré prevádzkujú ich ekonomiku, sa podľa odborníkov v týchto stratégiách považovali za zvlášť zraniteľné voči kybernetickým, vojenským útokom.

Obavy z medzinárodných právnych obmedzení v oblasti kybernetickej vojny však odradili amerických vládnych hackerov od plného využitia ich možností. Pentagon uviedol, že burzy, bankové systémy, univerzity a podobné civilné infraštruktúry nemôžu byť napadnuté len preto, že sa to dá. Podľa princípu vojenskej nevyhnutnosti, musí byť preukázaná určitá očakávaná vojenská výhoda. (Frontline, 2016; Arkin 1999)

2.3 ÚTOK NA ESTÓNSKO 2007

V apríli a v máji 2007 hackeri odštartovali vlnu kybernetických útokov, ktoré estónske úrady vyhodnotili ako „on line násilie" riadené Kremľom. Tento útok mal byť dôsledkom rozhodnutia Estónska presunúť sovietsky pamätník Druhej svetovej vojny z centra hlavného mesta na vojensky cintorín na predmestí, čo vyvolalo zúrivé protesty ruskej vlády a nepokoje v ruskej etnickej menšine v Estónsku.

Od samého začiatku obviňoval estónsky minister zahraničných vecí Urmas Paet z týchto útokov Putinovu vládu. „Európska únia je napadnutá, pretože Rusko útočí na Estónsko," uviedol. (Davis 2007) Estónsko bolo v čase útoku európskym lídrom v elektronizácii procesov a v internetovom sieťovaní, čo odrážala aj populárna prezývka tohto malého pobaltského štátu - „eStonia". Odborníci uviedli, že stovky tisíc počítačov boli použité v koordinovanom útoku proti vládnym agentúram a bankám. Týmto masívnym kybernetickým útokom hackeri zablokovali vládnu komunikáciu, vládnu ekonomickú infraštruktúru, ale aj webové stránky novín, telekomunikačných spoločností, bánk a mediálnych oddelení vlády. Hranice Estónska nehlásili žiaden vpád, vzdušný priestor bol neporušený, útok (botnet) vkĺzol do krajiny cez najmenej chránenú hranicu - internet. Cely útok tvorený viacerými fázami a vo viacerých rovinách trval 2 týždne.

Útoky mali ďalekosiahle dôsledky nielen v Estónsku, ale v celej Severoatlantickej Aliancii, pretože mnohí odborníci sa domnievali, že útoky na Estónsko (ako členskú krajinu NATO) mohli byť iba testom. Aliancia vtedy ani nemohla využiť obranu proti takémuto obliehaniu, keďže vlády nemali kontrolu nad internetom, nemohli účinne bojovať proti takejto vojne na vlastnú päsť. Tieto udalosti podnietili NATO, aby posilnilo svoje kybernetické schopnosti a vytvorili v roku 2008 centrum výskumu počítačovej obrany Aliancie v Talline. Takisto vytvorili tlak na Európsku úniu, aby sa počítačové útoky stali trestným činom. Vojakov tak v tomto boji nahradili počítačoví experti. (Davis 2007)

2.4 ÚTOK NA IRÁNSKY NUKLEÁRNY PROGRAM

V januári 2010 si inšpektori Medzinárodnej agentúry pre atómovú energiu, ktorí navštívili iránsky závod na obohacovanie uránu v Natanze všimli, že výkonnosť centrifúg používaných na obohacovanie uránu sa drasticky zhoršila. Samotní inšpektori a ani iránsky technici, ktorí menej funkčné centrifúgy nahrádzali novými nevedeli, čo to mohlo spôsobiť. O päť mesiacov neskoršie výskumníci našli v jednom zo systémov škodlivé dáta a objavili tak prvú zbraň digitálnej povahy (Zetter, 2010).

Je všeobecne známe, že operácia Stuxnet poškodila centrifúgy používané v procese obohacovania uránu zmenou rýchlosti ich rotora. Vibrácie a deformácie spôsobené veľkými a

náhlymi zmenami rýchlosti zničili podľa publikovaných odhadov približne tisíc odstrediviek. Keďže ich Iránci nedokázali rýchlo nahradiť, museli vyrábať menej obohatený urán ako pôvodne zamýšľali. Útočníci manipulovali aj s procesnými hodnotami v riadiacej jednotke. Hoci bol tlak v odstredivkách oveľa vyšší, ako mal byť, systém hlásil prevádzkovateľovi štandardné hodnoty. (Lipovsky 2017) Stuxnet poškodil centrifúgy a spomalil proces obohacovania uránu v iránskom meste Natanz, čím oddialil proces výroby nukleárnych zbraní Iránom a to je nepochybne významný zásah do geopolitickej situácie a globálnych pretekov v zbrojení.

Osobitosťou spomínaného malvéru je, že bol navrhnutý neútočiť na počítačové systémy a siete. Infikoval len špecifické ciele, hlavne softwéry Siemens zodpovedné za monitorovanie a chod centrifúg. Špecifickom je aj jeho samotná povaha, pretože na rozdiel od dovtedy odhalených malvérov špionážnej povahy, Stuxnet bol prvým kybernetickým nástrojom schopným fyzicky ovplyvniť svoj cieľ a dnes sa preto považuje za prvú kybernetickú zbraň geopolitického významu (Macková, 2013). Krátko po odhalení malvéru Stuxnet boli identifikované aj ďalšie, ktoré patria do tejto „rodiny“ malvérov, ako napr. Duqu a Flame.

ZÁVER - KONIEC V NEDOHĽADNE

Rusky expert na kybernetickú bezpečnosť Andrej Soldatov upozorňuje na to, že „kybernetický experti, najmä armádni, sa stále snažia konať podľa schémy, ktorá naznačuje, že aktéri sú vojenskí a že kybernetické útoky udierajú na vojenské ciele. Mnoho rokov pretrvával boj medzi ruskou totalitnou terminológiou a západnou terminológiou o používaní pojmu kybernetická bezpečnosť alebo bezpečnosť informácií. Západná terminológia uprednostňuje kybernetickú bezpečnosť, pretože hovorí najmä o počítačoch, sieťach, hackingu, kým ruskí generáli vždy hovorili o obsahu informácií.” Preto sa v ruskej doktríne informačnej bezpečnosti od samého začiatku (od roku 2000) spomínali nepriateľské činy zahraničných médií. (Medvedev 2017) Podľa expertov na bezpečnosť sa efektívnosť vplyvu informácií stáva úmernou k účinkom vojenských prostriedkov. Okrem toho politicky a diplomaticky tlak, embargo, obchodno-ekonomické vzťahy, protekcionistické opatrenia a kvóty sa stávajú nástrojom podpory pre následné silové riešenia. Takéto komplexné opatrenia jednoznačne zapadajú do rámca súčasného fenoména, ktorý sa nazýva „hybridná vojna”. Tieto vojny výrazne rozširujú škálu hrozieb a stávajú sa jedným z hlavných spôsobov dosahovania vojensko-politických a strategických cieľov. Hybridná vojna vo svojej podstate integruje celú škálu bojových prostriedkov – od najmodernejších a technologicky vyspelých (kybernetická vojna a informačná konfrontácia) až po využitie primitívnych teroristických metód a taktík pri vedení ozbrojeného konfliktu.

Tieto prostriedky spája jediný zámer a cieľ zameraný na zničenie štátu, podkopanie jeho ekonomiky a destabilizáciu vnútornej spoločensko-politickej situácie. Správy o cielených útokoch a „sponzorovanom malvéri” (malvér, za ktorým stojí vláda alebo iný subjekt) otvorili globálnu diskusiu o spôsoboch využívania malvéru. (ESET 2016) Mnoho výskumníkov v USA predáva svoje exploity vláde, vrátane špionážnych agentúr. Využívanie týchto exploitov na masy užívateľov internetu však vyvoláva kontroverzie. Dňa 5. novembra 2016 televízia NBC oznámila, že hackeri pracujúci pre americkú vládu získali prístup k ruskému energetickému systému a ďalším prvkom kritickej infraštruktúry. (Brewster 2016)

Koncom roka 2016 priniesli médiá v Spojených štátoch sériu správ o tom, že časti kritickej infraštruktúry USA sú penetrované skrytými malvérmi z Ruska, Číny a ďalších krajín. Rovnako informovali, že americkí vojenskí hackeri penetrovali ruskú distribučnú sieť elektrickej energie, telekomunikačné siete a veliteľské systémy Kremľa, zraniteľnosťami voči

útokom tajných amerických kybernetických zbraní. Takáto vzájomná penetrácia všetkých strán sa podľa americkej televíznej stanice NBC javí ako príprava na „totálnu kybernetickú vojnu". (Sputniknews, 2016)

Programy „kybernetickej vojny" predstavujú vážnu hrozbu proliferácie, pretože nie je možné udržať kybernetické zbrane na rozdiel od iných typov zbraní pod účinnou kontrolou. Kybernetické zbrane sú v skutočnosti len počítačové programy. Možno ich kopírovať rýchlo a takmer bez nákladov.

Nekontrolované šírenie kybernetických zbraní v dôsledku neschopnosti ich ovládnuť v kombinácii s ich vysokou trhovou hodnotou je porovnateľné s globálnym obchodom so zbraňami. Globálny „trh počítačových zraniteľností" poskytuje vládnym hackerom značnú finančnú motiváciu kopírovať a predať kópie kybernetických zbraní za státisíce až milióny dolárov. Takéto zbrane môžu využiť akékoľvek spoločnosti na priemyselnú špionáž alebo získanie prevahy nad konkurenciou.

Koncom roka 2016 prezident Ruskej federácie Vladimir Putin uviedol, že „Rusko je teraz silnejšie, než ktorýkoľvek potenciálny agresor" a vyjadril tiež potrebu rýchleho prispôsobovania plánov na neutralizáciu potenciálnych hrozieb voči Rusku vrátane modernizácie armády. (U.S.news, 2016)

Preteky v kybernetickom zbrojení medzi Ruskom a USA by mohli pripomínať vznik „Novej éry Studenej vojny", ale je to mylný názor, pretože v tejto hre sú aj ďalšie veľmoci (EÚ, Južná a Severná Kórea, Čína).

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ARKIN, W. M. 1999: *The Cyber Bomb in Yugoslavia.* [on-line]. Dostupné na internete: Washingtonpost.com: dot.mil

BREWSTER, T. 2016: *Meet the Russian Hacker.* [on-line]. Dostupné na internete: Meet The Russian Hacker Claiming She's A Scapegoat In The U.S. Election Spy Storm (forbes.com)

CLAUSEWITZ, C. 1996. *O válce.* Nakladateľstvo Bonus A, s.r.o. Druhé vydanie, Brno 1996. ISBN 80-85194-27-1. 756 s.

DAVIS, J. 2007. *Hackers take down the most wired country in Europe*. [on-line]. Dostupné na internete: Hackers Take Down the Most Wired Country in Europe | WIRED

IVANČÍK, R. 2020. Manažment bezpečnosti a obrany: Rast významu ochrany kritickej informačnej infraštruktúry pred kybernetickými útokmi na úrovni štátu i na úrovni Severoatlantickej aliancie. *Vojenské reflexie: Vojenský vedecký časopis [online]. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, ročník XV., č. 2/2020.* ISSN 1336-9202. S 45-62. Dostupné na internete: vojenske_reflexieXV_2.pdf (aos.sk)

JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. 2013. Výkladový slovník kybernetické bezpečnosti. Policejní akadémie ČR, Praha, 2013. ISBN978-80-7251-397-0. 197 s.

JURČÁK, V. 2020. Prolegomena. In : Teoretické prístupy k skúmaniu bezpečnosti. Monografia. KEY PUBLISHING s. r. o., 2020. 134 s. ISBN 978-80-7418-358-4.

LIPOVSKY, R. 2017: Seven years after Stuxnet: Industrial systems security once again in the spotlight. [on-line]. Dostupné na internete: Seven years after Stuxnet: Industrial systems security in the spotlight again (welivesecurity.com)

MACKOVÁ, V. 2013. Cyber War of the States: Stuxnet and Flame Virus OpensNew Era of War. In CENNA Policy Papers. Centre for European and North Atlantic Affairs, Bratislava, 2013, vol. 2 no. 15.

MEDVEDEV, S. 2017: Medvede za klávesnicou. [on-line]. Dostupné na internete: Медведи за клавиатурой (svoboda.org)

RUBANOV, V. 2017: Hackerov nejde deliť na svojich a cudzích. [on-line]. Dostupné na internete: An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED

ŠIMONOVÁ, M. 2021. Kybernetická bezpečnosť – analýza legislatívneho prostredia Slovenskej republiky a aktivít na národnej a medzinárodnej úrovni. Vojenské reflexie: *Vojenský vedecký časopis* [online]. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2021, **16** (1), 126 s. ISSN 1336-9202. S 47-60. DOI: https://doi.org/10.52651/vr.a.2021.1.47-60

ZETTER, K. 2010. An Unprecedented Look at Stuxnet, the World' First Digital Weapon. The Wired. Dostupné na internete: An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED

Computerr attacks at department of defence. Frontline, 1996. Dostupné na internete: The Risks - Computer Attacks At Department Of Defense Pose Increasing Risks | Hackers | FRONTLINE | PBS

Target: Yugoslavia (A Look into the Future). Consortium News, 2016. Dostupné na internete: Target: Yugoslavia (A Look into the Future) (consortiumnews.com)

US Military Hackers Claim Penetration of Russian Infrastructure. Sputnik 2016. Dostupné na internete: US Military Hackers Claim Penetration of Russian Infrastructure - 05.11.2016, Sputnik International (sputnikglobe.com)

Putin Says his Army is Best. U.S. News, 2016. Dostupné na internete: Vladimir Putin: Russia's Military Is Stronger Than Any Potential Foe (usnews.com)

ESET 2016: Trends for 2016: Insecurity everywhere. [on-line]. Dostupné na internete: eset-trends-2016-insecurity-everywhere.pdf (esetstatic.com)

The First Computer Virus of Bob Thomas Explained: Everything You Need to Know (1971).Dostupné na internete: The First Computer Virus of Bob Thomas (history-computer.com)

Záväzok v oblasti kybernetickej obrany. Varšavský summit NATO, 2016. Dostupné na internete: NATO - Oficiální text: Závazek kybernetické obrany, 8. července 2016

prof. Ing. Vojtech JURČÁK, CSc.
Demänová 393, Akadémia ozbrojených síl generála Milana Rastislava Štefánika
e-mail: vojtech.jurcak@aos.sk

doc. Ing. Vladimír ANDRASSY, PhD.
Demänová 393, Akadémia ozbrojených síl generála Milana Rastislava Štefánika
e-mail: vladimir.andrassy@aos.sk

Mgr. Katarína STOLÁRIKOVÁ, PhD.
Inštitút pre národnú a medzinárodnú bezpečnosť
e-mail: kata.stolarikova@gmail.com