PhDr. Antonín Rašek

Kybernetická válka pokračuje

INFORMACE

Na kybernetické hrozby a možnost kybernetické války neexistuje jednotné mínění, což je u nových jevů obvyklé. Hrozby se netýkají jen vládních institucí, ozbrojených složek, ale i ekonomických organizací a následně či přímo jednotlivců. Ekonomická bezpečnost je přitom neméně důležitá jako přímé vojenské ohrožení. Nemluvě o tom, že v bezprostřední budoucnosti lze předvídat prioritu ekonomických střetů před násilnými. V tomto textu převažuje sociologický pohled a cílem je hledat především sociální souvislosti a důsledky kybernetického potenciálů, a proto se nevyhýbá sekundárním zdrojům informací, ke kterým se většina čtenářů převážně dostává. Záměrem je vyzvat odborníky ITT, aby se k této problematice vyslovili profesionálnějším využitím primárních zdrojů informací jakými jsou např. studie společností Symantec a McAfee k hrozbám Stux NET a DuQu, zprávy CSIRT a CERT týmů, analýzy a zprávy amerického GAO pro Kongres USA a další.

Z vojenského hlediska je zřejmé, že kybernetické útoky a obrana proti nim musí být integrální součástí ozbrojených aktivit. Je tomu tak proto, že vojáci považují internet a virtuální prostor jako pátou oblast nasazení svých sil vedle země, vzduchu, vody a vesmíru. Armády začínají budovat speciální jednotky, některé státy jim k tomu vytváří příslušný právní a politický prostor, jak je tomu v případě americké směrnice k boji proti kybernetickým útokům. Příkladem využití prostředků „kyberválky" je např. použití počítačového viru Stuxnet proti Íránu, který napadl počítače v jaderném zařízení v Búšehru.

Výrazně se zvyšující počet kybernetických útoků, jejich sofistikovanost a výše škod i přes zlepšující se obranná opatření, nasvědčuje tomu, že varování před vypuknutím skutečné kybernetické války dokonce v globálním rozsahu, není již science-fiction, divokou kartou nebo černou labutí. [1] Kybernetická bezpečnost se postupně stává jednou z priorit národních bezpečnostních politik a mezinárodní agendy organizací, jako je Severoatlantická aliance a Evropská unie. Není nemožné, že se jednou stane prioritou hlavní.

Spolu s tím je proto nezbytné zabývat se tím jak tato hrozba ovlivní psychiku vojáků i civilního obyvatelstva a jaké může mít sociální důsledky, jak může ovlivnit reakce obyvatelstva.

Získávat zprávy a ovlivňovat nepřátelské spojovací systémy se podle Vladimíra Bäumela [2] začalo ve značném měřítku používat již v době druhé světové války a značných rozměrů tento boj dosáhl v dobách války studené (např. REB – radioelektronický boj).

Logika problematiky podle názoru Jaroslava Štefce [3] napovídá, že pokud se kybernetika týká na jedné straně organizace procesů a informačních toků u živých organismů a na druhé straně u strojů a ve společenstvích, přímo se nabízí paralela s terminologií spojenou se zbraněmi hromadného ničení (ZHN), konkrétně s biologickými a částečně

i chemickými zbraněmi. Koneckonců precedenty tu již jsou – počítačové viry a virové útoky, léčení virové nákazy, uzavření zavirovaného souboru do virového trezoru nebo „karantény“, antiviry apod. Možná by stálo za úvahu zahrnout „kybernetické zbraně“ mezi ZHN – způsobená škoda může být nevyčíslitelná. Majetek zůstává, stejně jako při použití neutronové pumy, zatímco lidé vymírají v důsledku krachu systému dopravy a zásobování potravinami, vodou a energiemi, postaveném na lehce zranitelném systému digitálního přenosu a zpracování dat atd. Terminologie se bude muset teprve vytvořit a ustálit.

Kybernetická válka nebo zkráceně kyberválka je podle některých institucí a expertů vyústěním kybernetického terorismu. Terminologický slovník ji definuje jako: „Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem, je tzv. kyberprostor… a prováděné prostřednictvím počítačové sítě.“ [4]

Zužovat kybernetické útoky jenom na kyberterorismus by logicky bylo chybné. Boj proti terorismu a terorismus samotný je velmi složitým jevem, který je determinován mnoha faktory, je to i reakce na globalizaci. Kybernetické útoky mají mnoho forem a příčin, přičemž teroristických je zatím jen malé procento. Útoky se odehrávají mezi státy, ekonomickými a bezpečnostními aktéry, mezi státem a soukromým sektorem, mezi kriminálním světem a soukromým sektorem atd. Celkový systém fungování států, firem, armády, kosmu, komunikace a financí je postaven na informačních systémech. Proto bude tato oblast nejvíc ohrožovanou. Zatím jí ale není věnovaná dostatečná pozornost. [5]

Kybernetické nástroje mohou v budoucnosti výrazně změnit geopolitické rozložením sil. K prostředkům útoku vedeného počítači se dostávají i jednotlivci. Stáhnout si z webu postup na vytvoření počítačového viru nebo návod na vyřazení serverů je podle expertů ITT relativně jednoduché. Neznamená to, že jsou s nimi okamžitě schopni ohrozit tak sofistikované systémy, jaké mají moderní státy a armády. [6] **Je zřejmé, že bude nutné odlišit kyberválku s jasnými politickými a vojenskými záměry, motivy a cíli, od počítačové kriminality, jakkoli jsou zčásti provázané a technicky spolu souvisejí.** Na to upozornila i mezinárodní konference Cyberterrorism: Tackling Political Aspects of Cybersecurity, která se konala 6.–7. 12. 2011 v Praze. [7]

První zkušenosti s vedením kybernetických válek

Podle zprávy společnosti McAfee velké země již v „kybernetické studené válce“ zapojeny jsou: navzájem se špehují a testují své sítě. Studii vedl bývalý poradce Bílého domu pro národní bezpečnost Paul Kurtz a přispělo do ní přes dvacet expertů z mezinárodních vztahů, národní bezpečnosti a internetové bezpečnosti. [8]

Zkušenosti s využitím praktik kybernetické války získali Američané např. při ochromení irácké obrany v Iráku. Dlouho chyběla zejména možnost identifikace nepřítele. V Evropské unii se sice tato agenda na pořad dostala, ale ne v takové intenzitě jako ve Spojených státech.

Kybernetické útoky se vedou i ve vojenské oblasti. Počítačové viry jsou schopny napadnout i americká bezpilotní letadla. Ovládací systémy amerických bezpilotních letounů, které působí v Afghánistánu i v dalších bojových oblastech, počítačový virus již napadl. Podle serveru Wired.com, který se odvolal na armádní zdroj, virus neznamená překážku pro další mise letadel, není ale vyloučeno, že by mohl způsobit únik tajných vojenských informací.

Koncem roku 2011 Írán oznámil sestřelení amerického bezpilotního letadla nad svým územím. Spojené státy nejprve tvrdily, že o ničem takovém nevědí, později spolu se Severoatlantickou aliancí přiznaly, že jeden dálkově ovládaný výzvědný letoun v Afghánistánu opravdu postrádají. Podle nich měl technickou závadu. Usuzuje se, že nešlo o sestřelení, ale nejspíš se Íráncům podařilo změnit dráhu jeho letu a následně přistál na íránském území, protože bezpilotní letoun nebyl poškozen. [9] Je zřejmé, že jde o velmi sofistikovanou záležitost, kterou jsou schopny realizovat jen velmi zkušené týmy počítačových expertů. Lze se proto domnívat, že nejde o samostatnou íránskou aktivitu, ale byla nejspíš provedena za spolupráce jiných zemí, nejspíš Číny nebo Ruska. Už jen tato podezření mohou narušovat mezinárodní vztahy.

Virus pronikl i do počítačů na letecké základně Creech v Nevadě, odkud se řídí lety bezpilotních letadel typu Predator a Reaper. Napadl počítače, na nichž se pracuje s utajenými údaji. Virus zaznamenává všechny úhozy do klávesnice a není vyloučeno, že je posílal svému zatím neznámému tvůrci. Armáda údajně zatím nevěděla, zda byly řídicí systémy bezpilotních letadel napadeny úmyslně nebo zda se do nich virus dostal náhodně při prohlížení internetových stránek. Problémem je, že se nedaří škodlivý software z počítačů odstranit. [10]

Bezpilotní letouny přitom patří mezi hlavní technické výhody USA ve válkách, které vedou. Americké armádě v Afghánistánu slouží asi 150 letadel k průzkumu terénu i jako prostředek k útoku na pozice povstalců z hnutí Talibán. Americká Ústřední zpravodajská služba (CIA) je využívá k náletům na úkryty Talibánu a teroristické sítě Al-Ká'ida v pákistánském pohraničí; během posledních dvou let takových útoků podle listu The Washington Post provedla přes 230.

Američané nasadili bezpilotní letadla i do bojů v Libyi, kde s nimi provedli přes 90 náletů. Letoun tohoto typu také koncem září 2011 zlikvidoval šéfa jemenské odnože Al-Ká'idy Anwara al-Awlakiho.

Malware údajně pronikl i do počítačů amerického letectva, které odpovídají za řízení letového provozu Predator a Reaper. Přes veškerou snahu se údajně škodlivé kódy nepodařilo zcela zlikvidovat. [11]

Ohrožena mohou být i pilotovaná letadla včetně vojenských, např. i zakoupeným hardwarem. Virus hardwaru údajně nemá vliv na fungování letadla, ale zaznamenává činnosti pilota. Vzhledem k tomu, že vojenská síť je izolována od veřejného internetu, shromážděné informace nebude malware moci nikomu předat. Nelze však na to spolehat, když virus do systému dokázal proniknout, najde možná cestu i opačným směrem. Spekuluje se, že malware byl už přítomen na pevném disku nebo jiné komponentě, která byla připojena do vojenské sítě. Proto čipy vyrobené v cizích zemích, především firmami z východní Asie, představují pro vojenské systémy riziko. Armáda nejspíš bude muset mít vlastní výrobce hardwaru. [12]

Hackeři jsou schopni napadnout i satelity NASA. Stalo se tak v roce 2007 a 2008. Podle agentury Bloomberg se podařilo hackerům na několik minut ovládnout její dva satelity. Mohli vysílat i přijímat data, ovládat jejich pohyb na orbitě a v krajním případě je dokonce nechat spadnout. O obou útocích pojednává pravidelná zpráva o ekonomických a bezpečnostních vztazích mezi Amerikou a Čínou. Její kopii se podařilo agentuře Bloomberg získat.

Podobně je u strategických raketových systémů a v protiraketové obraně, kde hrozí vyřazení naváděcích systémů. Např. bývalý ruský prezident Medveděv ve zprávě

o vývoji prostředků, které by měly působit na naváděcí systémy amerických antiraket, mj. zmiňuje i katastrofický scénář toho, jak by průnik hackerů do systémů NASA mohl vypadat: „Takový průnik představuje řadu potenciálních hrozeb, zvláště je-li dosaženo na satelity s více citlivými funkcemi. Přístup k ovládání by útočníkovi umožnil satelit poškodit, nebo zcela zničit."

Podle zprávy se podařilo hackerům ovládnout satelity přes internet pomocí infikovaných počítačů na základně Svalbard v norských Špicberkách. První průnik byl zaznamenán v říjnu 2007, kdy počítačoví piráti získali nadvládu nad satelitem Landsat-7, který monitoruje povrch Země, na více než 12 minut. Druhým napadeným satelitem byl v červnu 2008 Terra AM-1, který slouží ke studiu klimatu. Ten hackeři ovládali dvakrát dvě minuty. Co přesně v inkriminovanou dobu hackeři se satelity dělali, zpráva nezmiňuje. Jisté ani není, odkud přesně útoky hackerů pocházely. Podle jedné z teorií mohlo jít o Čínu. Tamní vláda jakoukoliv spojitost s průniky popírá. [13]

Posledním příkladem využití prostředků kyberválky může být použití počítačového viru Stuxnet proti Íránu, které bylo podle deníku New York Times izraelským dílem. Írán potvrdil, že Stuxnet napadl soukromé počítače v jaderném zařízení v Búšehru, ale nezpůsobil tu žádné vážné škody. Podle počítačových odborníků byl tento nevídaně propracovaný malware prvním odhaleným virem zacíleným na průmyslové řídicí prvky. Mnozí experti tvrdili, že za tak složitým programem musí stát „nějaký stát". Zatímco první domněnka expertů na bezpečnost v kyberprostoru se potvrdila, druhá zůstává spekulací. Írán sice oznámil zadržení blíže nespecifikovaného počtu špionů, možného původce útoku však nejmenoval. [14] Počítačový virus Stuxnet prý nechal nasadit proti íránskému jadernému programu prezident USA Barack Obama. Chybou programování se technologie vymkla kontrole a rozšířila se i na webu.

Kybernetická aktivita proti Íránu pokračovala, když se v počítačových sítích objevil virus podobný viru Stuxnet pod názvem DuQu, proti němuž podle sdělení představitele civilní obrany Golamrézá Džalálího byl firmou Symantec vytvořen obranný software, i když zároveň přiznal, že dostatečně nevědí, kam tento virus pronikl. Útok pokračoval virem Stars. Íránci se domnívají, že za viry jsou Izraelci nebo Američané. [15] Virus údajně roztočil odstředivky do tak vysokých otáček, až došlo k jejich poškození. Oklamal i obsluhu. Na monitorech uváděl běžné údaje o provozu z minulých dní, a oni do poslední chvíle neměli o postupné destrukci svých zařízení ani ponětí. [16]

Na trojského koně označovaného DuQu upozornili výzkumníci ze společností Symantec a McAfee. Trojan má být navržen tak, aby výrobcům průmyslových řídicích systémů kradl informace z projektové dokumentace, které pak lze zneužít pro tvorbu dalších útočných kódů (Symantec). DuQu může také provádět cílené útoky na weby typu certifikačních autorit (McAfee). Nový malware vytvořili buď přímo tvůrci Stuxnetu, nebo měli alespoň přístup k jeho zdrojovému kódu. Se Stuxnetem má sdílet řadu vlastností; není naprogramován k sebereplikaci a aby po sobě smazal stopy, z infikovaného systému se sám odstraňuje.

Koncem května 2012 odborníci z ruské firmy Kaspersky Labs odhalili pravděpodobně nejkomplexnější odcizení digitálních dat. Malware Flame možná již v roce 2007 nebo je později v roce 2010 infikoval tisíce počítačů v Izraeli, Íránu a na Středním východě a jehož původce se nepodařilo identifikovat. Je důkazem stále sofistikovanějšího vedení kybernetické války. Flame přinejmenším dokáže na dálku měnit nastavení počítače, aktivovat mikrofony na PC a nahrávat konverzaci v okolí,

odposlouchávat konverzaci přes chat i snímat obrazovku. [17] Vývoj Flame údajně stál miliardu USD.

Během leteckých útoků proti Kaddáfího režimu USA prý zvažovaly možnost narušit kybernetiky systémy libyjské protivzdušné obrany. Americká administrativa i armádní představitelé nakonec tuto možnost zavrhli, aby nevznikl precedent a podobné postupy pak nezačaly otevřeně používat i jiné země jako Rusko a Čína. Nikdo si také nebyl jistý, zda má prezident USA pravomoc kybernetické útoky nařídit bez toho, aby o svém postupu neinformoval Kongres.

Už i při likvidaci bin Ládina se údajně uvažovalo o menší akci, která by zaslepila pákistánské radary. Na konec od tohoto postupu bylo i tehdy upuštěno.

Společnost McAfee a organizace CSIS (Center for Strategic and International Studies) zveřejnily výsledky průzkumu, který mapuje škodu a dopad kybernetických útoků na kritickou civilní infrastrukturu, například na elektrorozvodné sítě nebo na systémy pro rozvod a zpracování pitné vody, ropy a zemního plynu. Průzkum mezi 200 zaměstnanci (s výkonnou pravomocí odpovědní za zabezpečení IT) firem z těchto sektorů ve 14 zemích vedl ke zjištění, že 40 % pokládá míru zranitelností ve svém oboru za stále se zvyšující. Téměř 30 % dotazovaných uvedlo, že jejich firma není dostatečně připravena na kybernetický útok. Více než 40 % očekává, že k masivnímu útoku dojde v průběhu následujícího roku. Téměř polovina respondentů z elektrárenského průmyslu objevila ve svých systémech červ Stuxnet. [18]

Podle expertů z průzkumu vyplynulo, že řada systémů kritické infrastruktury se opírá o nedostatečně chráněné počítačové sítě. Kybernetické útoky proti těmto sítím způsobily obrovské škody. Stejně tak představuje bezpečnostní hrozbu i neregulovaná ekonomika a spekulativně fungující bankovní systém. [19]

Vážnost kybernetických hrozeb si nejvíce uvědomují Američané. Americká vláda podle agentury Bloomberg tajně vyšetřovala, zda v telekomunikačních sítích nejsou instalována cizí hardwarová a softwarová zařízení, např. čínská či jiná, která by monitorovala citlivé informace nebo dokonce vytvářela vhodné podmínky pro potenciální kybernetický útok. [20]

Je samozřejmě možné považovat tyto jevy za jednotlivé a dokonce izolované incidenty. Ale v některých případech lze již vysledovat cílené a cílevědomé úsilí využívat i jiné prostředky než tomu bylo v dosavadních ozbrojených střetnutích. Nemluvě o tom, že taková střetnutí je možné vést jako mnohdy v minulosti bez formálního vyhlášení války, takže může být i těžké identifikovat, pokud nepůjde o vyloženě strategický útok, zda vůbec cílevědomý útok začal. Podobně bude pro a psychology a sociology složité identifikovat psychické a sociální dopady na vojáky a civilisty a na základě těchto poznatků je i na takovou možnost účinně připravovat.

Kybernetické hrozby se nevyhýbají ani naší zemi a mnoha dalším

Koncem roku 2010 hackeři mnoha tisíci fiktivních objednávek vyřadili objednávkový systém České pošty právě v době, kdy byla zahlcena předvánočními nákupy. Hackeři zablokovali i jiné systémy počítačů a odcizili cenné informace mnoha institucí včetně vládních.

Roku 2011 organizovaný gang rumunských hackerů ukradl z českého elektronického registru emisní povolenky za zhruba 450 milionů Kč. ČEZ, a tedy i stát, přišly o 700 tisíc povolenek a investiční společnost Blackstone Global Ventures o 475 tisíc. O den později zastavila proto Evropská komise obchodování s emisními povolenkami v celé EU. Peníze sice byly zajištěny, ale tento případ ukázal, jaké možnosti má elektronický zločin a jaké škody může způsobit. [21]

Zřejmě největší kolaps přístupu k účtům přes internet trval pět hodin a došlo k němu u České spořitelny (ČS) na konci května 2010. Nefungoval web banky ani klientská linka. Pocítit to mohlo až milion uživatelů. Důvodem zřejmě bylo přetížení systémů. U plánovaných odstávek přímého bankovnictví byli klienti podle ČS vždy v předstihu informováni a nedošlo ke ztrátám dat ani peněz. ČS se ale vyhnula odpovědi na otázku, kolik případů neočekávaných výpadků internetového bankovnictví ročně eviduje. „Počty výpadků za rok kvantifikovat lze, ale čísla nemají valnou vypovídací hodnotu." [22]

Kybernetický útok si lze přes internet údajně i objednat. Takové služby nabízí například nájemná skupina hackerů pod označením H4H (Hackers-4-Hire). V nabídce jsou jak drobné kriminální delikty, tak rozsáhlé teroristické útoky. [23]

Vyspělejší společnosti jsou schopnější se bránit. „Předpokládá se, že kyberútoky budou stále intenzivnější a sofistikovanější," řekl ředitel odboru informační bezpečnosti na ministerstvu vnitra Aleš Špidla.

Podle Richarda Clarka, bývalého zaměstnance Bílého domu, který měl na starost boj s terorismem, postačí v budoucnu při promyšleně vedeném kyberútoku na vyřazení protivníka patnáct minut. Je to tedy válka na čtvrt hodiny. O tom si zastánci konvenčních operací mohou nechat jen zdát. Uvažuje se proto dokonce o zřízení speciálního soudního tribunálu pro počítačové útočníky. [24]

Hackeři z hnutí Anonymous odcizili z počítačů americké bezpečnostní poradenské firmy Stratfor 200 GB e-mailů a údajů o kreditních kartách jejích klientů včetně příslušníků americké armády a vojenského letectva, analytiků Goldman Sachs či MF Global. Cílem vánoční akce zároveň bylo odcizit milion dolarů (19,75 milionu korun) a rozdat je. V databázi osobních dat, kterou získala a zveřejnila hackerská skupina Anonymous po vánočním kyberútoku na počítače americké bezpečnostní poradenské firmy Stratfor, jsou také údaje o stovkách zaměstnanců NATO, tajných služeb a příslušníků armády. Na internetu jsou tak volně přístupné například e-mailové adresy a hesla úředníků, kteří pracují pro nejdůležitější britské vládní úřady a přicházejí do styku s citlivými informacemi. Útok hackerů z hnutí Anonymous na společnost Stratfor se odehrál 25. prosince 2011. [25]

Na internetu se také objevily kreditní karty statisíců Izraelců, které tam údajně poslali hackeři ze Saúdské Arábie. Podle izraelského webu ynetnews.com se terčem útočníků stalo 400 000 kreditních karet, z nichž podle izraelské centrální banky bylo jen 15 000 skutečně ohroženo. Podle izraelského webu byl útok zřetelně politicky motivován. Skutečnost, že hackeři zveřejnili údaje z kreditních karet k volnému použití, aniž by se sami chtěli obohatit, odhaluje podle odborníků na kybernetickou bezpečnost jejich pravé motivy. „Nejde o kybernetickou krádež, spíš o kybernetický terorismus," prohlásil Gadi Aviran z izraelské bezpečnostní agentury Terrogence Ltd. Izrael je poměrně častým terčem hackerů. Útoky, které přicházejí většinou z palestinského či obecně arabského prostředí, ale většinou nejsou příliš nebezpečné. [26]

V první desítce nejrozšířenějších hrozeb se objevily viry Scrinject.B. Gen, Iframe.B, Conficker, Autoit, Sality, Ramnit, TrojanDownloader.Iframe či PSW.OnLineGame. Jejich podíl se aktuálně pohybuje mezi 0,75 % a 2,40 %. [27]

Hackeři odcizili i kontakty britských poslanců. Jednou z obětí je baronka Emma Nicholsonová, která v rozhovoru s Guardianem incident odsoudila. „Dát všanc údaje o vládních úřednících je příšerně nefér. Úředníci v citlivých oblastech, jakými jsou obrana či armáda. mohou být dokonce vystaveni určitému nebezpečí. Chránit tahle data je opravdu hodně těžké, ale není to nemožné," řekla poslankyně. [28]

Odborníci na počítačovou bezpečnost varovali před virem, který ohrožuje uživatele elektronického bankovnictví. Virus SpyEve, který byl nedávno objeven, umožňuje počítačovým zlodějům vykrádat lidem účty a ještě po sobě maskovat stopy, napsal dnes zpravodajský server MSNBC. [29]

Virus se může dostat do počítače z nezabezpečených internetových stránek. Aktivuje se v okamžiku, kdy se uživatel počítače připojí do internetového bankovnictví, a dokáže zaznamenat přihlašovací údaje, které odesílá zlodějům. Zároveň virus dokáže vytvořit falešnou zprávu od banky, v níž z uživatele vyláká čísla jeho platební karty.

Virus také vytváří kopii stránek, kterou zobrazuje uživateli počítače při dalším přihlášení do internetového bankovnictví. Umožňuje tak zakrýt stopy o ukradení peněz z účtu, ať už jejich přímým odesláním nebo pomocí ukradených údajů o platební kartě. Majitel účtu se tak o ukradení peněz dozví jen z výpisu z účtu, nebo pokud se do bankovnictví připojí z jiného počítače.

Podle firmy Trusteer, která se věnuje internetové bezpečnosti, virus oddálí okamžik, kdy se poškozený člověk dozví o napadení svého účtu. To umožní zlodějům zvýšit svůj zisk, protože jejich oběť později nahlásí zneužití účtu či karty a banka přístup k nim později zablokuje.

Podle poslední uveřejněné statistiky společnosti Eset je aktuálně nejrozšířenější počítačovou hrozbou na světě INF/Autorun. Jde o směs hrozeb šířících se přes vyměnitelná média, nejčastěji USB flešky a externí pevné disky. Vir již dokázal nakazit 4,38 % počítačů. Druhé místo patří malwaru Dorkbot (3,43 %), který se také šíří především přes vyměnitelná média a v počítači shromažďuje uživatelská jména a hesla, která uživatel vyplňuje na určitých webových stránkách. Všechna data pak malware odesílá útočníkovi přímo do počítače. INF/Autorun není názvem jedné rodiny škodlivého kódu, ale několika rodin, které napadají autorun.inf od různých autorů, na rozdíl od červů typu Conflicker apod., které pocházejí od jednoho autora nebo autorů.

Počítačová gramotnost lidí se neustále zvyšuje. Především proto vymýšlejí hackeři nové triky, které jim umožní propašovat škodlivé kódy do cizích PC. Před připravovanými hrozbami varovali bezpečnostní experti předních antivirových společností. K nejrozšířenějším hrozbám na webu budou v letošním roce patřit takzvané Black Hat SEO útoky. V jejich případě počítačoví piráti zneužívají zájmu lidí o aktuální informace a snaží se šikovnou optimalizací propašovat svoje podvodné internetové stránky na přední příčky vyhledávačů.

V kurzu hackerů jsou stále častěji chytré mobilní telefony, protože uživatelé jejich zabezpečení nevěnují přílišnou pozornost. Většina těchto přístrojů má přitom přístup na internet, kde si lidé pročítají e-maily, přihlašují se k sociálním sítím nebo k internetovému bankovnictví. Bezpečnostní výzkumník Esetu Sebastian Bortnik si myslí, že kvůli stále se zvyšující popularitě se pozornost tvůrců malwaru zaměří hlavně na operační systém

Android. „Nemusí to znamenat kompletní přesun malwaru na mobilní zařízení, naznačuje to však důležité změny v ekosystému kybernetického zločinu," myslí si Bortnik. [30]

Po analýze škodlivých kódů získaných z infikovaných mobilních zařízení bezpečnostní experti zjistili, že 30 procent všech hrozeb pocházelo z Androidu Marketu, SMS trojské koně tvořilo 37 procent mobilního malwaru a 60 procent vzorků škodlivého kódu neslo charakteristiky botnetu – to znamená, že takto nakažené přístroje mohl hacker ovládat na dálku.

Vrásky na čele expertům dělají také digitální certifikáty. Ty standardně slouží k ověřování autenticity webových stránek. V podstatě tento certifikát tedy ručí za to, že obsah stránky je důvěryhodný. Podvodné certifikáty většina prohlížečů neodhalí. Pokud se podaří počítačovým pirátům certifikát ukrást, mohou jej využít pro své podvodné weby, aby se na napadeném počítači tvářily jako důvěryhodné. I zkušený uživatel se pak může domnívat, že pracuje s legitimní stránkou. „Z pohledu uživatele jsou incidenty založené na únicích informací certifikačních autorit téměř neřešitelné a nezjistitelné. V těchto případech nepomůže ani technická vybavenost v podobě aktualizovaného systému a antivirového programu," upozornil Stančík. [32]

Certifikáty neslouží jen k ověření autenticity webových stránek, ale i jinému účelu – jednotlivé stránky nejsou podepisovány. Certifikát je možné použít pro podepsání domény (technologie DNSSec) nebo k zabezpečení webového sídla (SSL). Tedy umožňuje zjistit, jestli doména/webové sídlo patří skutečně deklarovanému majiteli, nebo se jedná o podvrh. Pokud útočník pozmění stránku na takto chráněném webu, na procesu ověření se to neprojeví. Většina moderních WWW prohlížečů obsahuje standardně nástroje pro kontrolu certifikátů, a tedy umožňuje odhalit podvodné certifikáty (poté co dojde k jejich revokaci). Problematika certifikátů je poměrně složitá a jedná se o problematické místo v zabezpečení komunikace na internetu.

Počítačoví piráti se stále častěji angažují mimo jiné v politice. Tento stále více se rozmáhající trend bezpečnostní experti nazývají *hacktivismus*, tedy aktivita hackerů v on-line světě. „Více než dříve budou tyto akce mířit proti politikům, soudům, policejním složkám, ale i vrcholným manažerům," konstatovala Hanibalová. [33]

„V roce 2012 dojde také k ukázkovým akcím v oblasti kybernetické války. Hlavním cílem zatím bude spíše testovat možnosti těchto útoků. Až dosud vlády vyspělých zemí chránily především své vládní a vojenské sítě. Nyní si bude třeba uvědomit i míru škod, které mohou způsobit akce proti další kritické infrastruktuře zejména rozvodným sítím," doplnila.

Ideologicky motivovaný útok zaznamenala společnost Eset například po prosincových parlamentních volbách v Rusku. Cílem hackerské aktivity se stala webová stránka Superjedi.ru, kde si v diskusním fóru lidé vyměňovali názory na politickou situaci v zemi, upozornil server Softpedia.

Zabránit se před ním mohou uživatelé poměrně jednoduše. „Pro zabránění šíření malwaru zneužívajícího soubor Autorun.inf stačí jen zakázat automatické spouštění vložených médií ve Windows, přičemž Windows 7 tuto možnost mají deaktivovanou přímo v základním nastavení," uvedli již dříve zástupci Esetu.

Zabezpečení počítačů stejně jako obezřetnost uživatelů jsou stále na vyšší úrovni. Proto se hackeři místo samotného operačního systému budou stále častěji soustřeďovat na ovládací programy jednotlivých komponent počítače – takzvané *firmwary*. „Tyto útoky sice nejsou snadné, ale v případě úspěchu umožňují podvodníkům vytvořit

malwarovou vrstvu na úrovni síťových karet nebo například pevných disků," konstatovala mluvčí společnosti McAfee Alžběta Hanibalová. [33]

Tento typ útoku přitom patří mezi nejzákeřnější, protože antiviry a firewally v operačním systému nedokážou tyto hrozby zachytit. Zkušenější uživatelé si mohou všimnout, že jejich počítač pracuje pomaleji a některé webové stránky se nenačítají zcela správně.

S nevyžádanou poštou se snaží bojovat snad každý uživatel, i proto její podíl neustále klesá. Aktuálně je sedm z deseti odeslaných e-mailů spam. Ještě loni to přitom byla každá devátá odeslaná zpráva. V letošním roce by měl internet zaplavit takzvaný legální spam.

„Množství spamu sice klesá, nicméně toto místo nyní zaplní inzerenti, kteří budou houfně používat seznamy adres, jejichž uživatelé dali k zasílání souhlas. Krachující firmy budou za tímto účelem prodávat databáze svých uživatelů," varovala mluvčí společnosti McAfee Alžběta Hanibalová. [33]

Fenomén legálního spamu se postupně rozšiřuje po celém světě. I v České republice se najdou firmy, které zasílají zákazníkům různá reklamní oznámení klidně i několikrát za den. Za podobná reklamní sdělení přitom firmy inkasují při dostatečném počtu příjemců i stovky tisíc korun.

Stále častěji se uživatelé budou setkávat s útoky na sociálních sítích, kdy se budou v příspěvcích objevovat falešné odkazy na zajímavá videa. Na první pohled nemusí uživatel vůbec poznat, že se ho někdo snaží podvést.

Útok začíná zpravidla tak, že od některého přítele přijde zpráva psaná v anglickém jazyce. V textu se podvodník ptá: „Jak se daří? Co děláš? Už jsi viděl tohle video na youtube?" Text je doplněn odkazem na avizované video.

Problémy nastanou ve chvíli, kdy uživatel na odkaz klikne. Je totiž vyzván k aktualizaci pluginu videopřehrávače internetového prohlížeče. Místo legitimního programu Adobe Flash Player si uživatel do počítače stáhl nebezpečný počítačový virus.

„Infikované počítače se stávají součástí botnetu na bázi peer-to-peer, tedy sítě infikovaných počítačů, jejichž výkon může být využit na různé nelegální aktivity hackerů," varoval loni Igor Hák ze serveru *Viry.cz*, kdy podobným způsobem počítačoví piráti cílili na uživatele Facebooku. [34]

Na začátku nového roku 2012 se objevila zpráva, že došlo k objevu počítačového viru k identifikaci původce kybernetického útoku, který zároveň ochromuje jeho program. [35] To by mohlo podstatně změnit situaci, jenže jak dobře víme z historie, na každý nový objev se vždy najde obrana.

Uvedené informace se převážně týkají civilního sektoru a jsou dílčí. Ale zároveň nelze přehlédnout, že se v nich získávají informace o formách zneužívání internetu a útocích na instituce a jednotlivce. Je logicky jen věcí času, kdy aktéři těchto procesů budou angažováni buď ve prospěch vedení kybernetických útoků a následně i vedení kybernetické války, či na obranu proti takovým záměrům. Lze předvídat, že již nyní mnoho států se připravuje jak na obranu, tak vedení kybernetických střetů, V Číně si pro takový záměr zřídili i speciální institut. [36]

Subjekty kybernetické hrozby

Klíčovými aktéry útoků jsou hackeři. Proti jejich aktivitám jsou přijímána stále tvrdší opatření i ve formě zákonů, jsou postihováni, zatýkáni, jak se to stalo např. ve Spojených

státech, a odsuzováni i k tvrdým trestům. Zčásti je to nerovný boj, útoky hackerů jsou relativně nenákladné, obrana proti nim mnohonásobně dražší.

Vážným problémem jsou osobnostní charakteristiky hackerů, zvláště jejich psychologický profil, proto lze těžko předvídat jejich záměry. Jejich zneužití pro vedení kybernetických útoků je proto vážnou bezpečnostní hrozbou.

Identifikace skutečných cílů odhalených kyberútoků je značně složitá. Nelze vyloučit ani možnost, že řada z nich byla učiněna jen jako krycí manévr, který měl odvést pozornost od skutečného pachatele. Ten ani nemusel mít strategické cíle a mohlo jít „jen" o ekonomickou špionáž. Tento faktor zdůraznil viceprezident firmy McAfee Dmitri Alperovitch, když pro CNBC uvedl: „Jednalo se o největší transfer bohatství duševního vlastnictví v historii." [37]

V této souvislosti dochází až k absurdním epizodám. Nový australský ministr obrany Stephen Smith využil při své první cestě do Číny nezvyklého postupu. Aby se nemusel bát, že ho velká země bude odposlouchávat, nechal on i jeho tým všechny mobily a laptopy už v Hongkongu. Paradoxem je, že čím technologicky vyspělejší technika se vyvíjí a zařazuje to provozu, tím vážnější je hrozba. Potvrzuje to ideu rizikové společnosti Ulricha Becka. [38]

O schopnostech hackerů alespoň jeden příklad. Slovinské policii se podařilo dopadnout počítačového piráta, který podle obvinění infikoval zákeřným virem 12 milionů počítačů. Ty zapojil do několika botnetů (sítě tzv. zotročených PC), které slouží k rozesílání spamu, k internetovým útokům a nelegálním činnostem. [39] Je zřejmé, že psychologický profil hackerů a jejich aktivity se musejí stát tématem sociálně-vědních výzkumů.

Reakce ve světě

Kyberútoky mohou být považovány za válečný akt, USA proto varovaly, že v případě kybernetického útoku na jejich vojenská zařízení nebo strategicky důležitá odvětví mohou zareagovat použitím síly. [40] Americké ministerstvo obrany připravilo strategii, jak v tomto případě postupovat. Má k tomu důvody. Pentagon uvádí, že tajné služby z více než stovky cizích zemí podnikají pokusy proniknout do počítačových sítí americké federální vlády i jejích největších vojenských dodavatelů. Příkladem je útok na informační systémy společnosti Lockheed Martin. K podobné akci došlo již v roce 2009, kdy hackeři pronikli do počítačů, v nichž byly informace o letounu F-35. USA odpoví na kyberútok silou, ale jen tehdy, pokud by výsledek takové počítačové sabotáže způsobil podobné škody jako fyzické napadení. Tedy kdyby důsledkem byly oběti na lidských životech, masivní materiální škody nebo kolaps celých životně důležitých sítí, například energetických. Problémem zůstává spolehlivá identifikace kyberútočníka. Ten sice může být vystopován např. v Rusku nebo Číně, ani poté ale nelze automaticky tvrdit, že jedná z rozhodnutí a na pokyn vlád těchto zemí.

Prezident Barack Obama na podporu těchto záměrů podepsal nařízení upravující pravidla kybernetických válek, které může americká armáda a tajné služby vést v zahraničí. [41] Prezidentský dekret stanoví, které operace musejí mít souhlas Bílého domu a jakými pravidly se mají řídit. Obamův výnos je vyvrcholením dvouletého úsilí amerického ministerstva obrany zanést pořádek do využívání kybernetického potenciálu.

Přichází zároveň v době, kdy USA začínají pracovat se svými spojenci na globálních pravidlech vedení počítačových válek. Podle AP jsou regule blízké pravidlům, která platí pro klasickou válečnou munici – od nasazení jaderných bomb až po elektronické sledování nepřítele. Směrnice Bílého domu například umožní vyslat testovací počítačový kód do sítě v cizí zemi, aby byla zjištěna její průchodnost. Experti tuto praxi přirovnávají k pořizování průzkumných satelitních snímků v reálném světě ke zjištění možných příštích cílů. [41]

Jak již bylo zmíněno, moderní armády začínají označovat internet a virtuální prostor jako „pátou oblast nasazení sil" vedle země, vzduchu, vody a vesmíru. Americká armáda, která je v současnosti technologicky nejvyspělejší, založila zvláštní United States Cyber Command (USCYBERCOM) a intenzivně se zabývá možnostmi elektronického vedení boje. [42]

V řadě zemí na obranu proti kybernetické hrozbě, hackerům a zemím zneužívajícím jejich služeb systematicky připravují a preventivně testují odolnost svých i cizích počítačových sítí. Evropská unie např. pro tyto účely zřídila agenturu ENISA.

Některé armády si vytvářejí zvláštní kybernetické jednotky; podobné aktivity organizují i zpravodajské služby. Objevují se hypotézy, že kybernetické aktivity mohou být neoddělitelnou součástí příštích vojenských střetnutí. Vážnou hrozbou je, že hackeři mohou kybernetické útoky vést sami.

Za nejvážnější hrozbu lze považovat internetovou „černou díru", tj. vytvoření sofistikovaného způsobu likvidace zasílaných životně důležitých informací, což by mohlo způsobit společenský, politický a ekonomický kolaps a vedlo k chaosu. NATO se proto rozhodlo **rozšířit možnost uplatnění článku 5 Severoatlantické smlouvy na útoky v kybernetickém prostoru**. To je u kybernetických útoků, jak bylo naznačeno, hůře realizovatelné, jejich původce bývá zpravidla odhalen až po dlouhé době, pokud vůbec. Je to však nutné, kybernetický útok může předcházet válce, jako tomu bylo v případě rusko-gruzínského konfliktu. Kybernetická hrozba má proto i vážné geostrategické důsledky, jimž je možné čelit spojeným úsilím takových organizací, jako je OSN, EU, NATO ad.

V souvislosti se Stuxnetem se Evropská unie rozhodla svou kybernetickou bezpečnost dále posílit. Její zástupci na konci října 2011 oznámili, že agentura ENISA zaměřená právě na počítačovou kriminalitu spojí své síly s Europolem. K posílení tohoto segmentu bezpečnostní politiky vyzvaly už v polovině září 2011 Evropu také USA. Náměstek ministra obrany William Lynn oznámil, že obě strany Atlantiku prohloubí spolupráci v této oblasti. „NATO má jaderný štít, buduje stále silnější obranný štít, potřebuje také kybernetický štít." [43]

Americké instituce údajně uvažují o tom, že by jako oficiální komunikační kanál mezi vládními agenturami mohly fungovat *smartphony* se systémem Android. Z tohoto důvodu byl iniciován projekt, jehož cílem je vyvinout speciální modifikaci jádra Androidu tak, aby systém byl bezpečnější a např. hardware mohl být jednoznačně spojen s konkrétní identitou uživatele. Systém musí pro dané použití získat patřičné certifikace. Pokud by výsledný kód byl uvolněn, našel by využití i jinde. Za jeho vývoj dosud odpovídají výzkumníci Googlu a George Mason University, výsledek by se měl objevit do dvou let. Až dosud se pro předávání zvlášť citlivých informací údajně používala rádiová komunikace. Americký prezident, členové vlády ad. spolu dosud komunikovali pomocí Black Berry. [44]

Ve Spojených státech v roce 2010 založili organizaci Cyber Command, která formálně spadá pod ministerstvo obrany. Jejím cílem je ochránit americké vojenské počítačové sítě a v případě potřeby i zaútočit na nepřátelské systémy. Rovněž Velká Británie má svoji vlastní kyberpolicii spadající pod Národní bezpečnostní agenturu. Německý Bundeswehr disponuje jednotkami, které se místo pořadových cvičení učí „klikat" myší a zadávat správné povely do klávesnice. Posílit vlastní kapacity kybernetické obrany je v horizontu příští dekády také jeden ze základních strategických cílů zemí sdružených v Severoatlantické alianci. Členské státy se na tom dohodly na summitu v Lisabonu. [45]

O tom, že to svět s bojem proti kybernetické hrozbě myslí vážně, svědčí i to, co řekl na odborném semináři ve sněmovně Pavel Fischer, ředitel politického odboru ministerstva zahraničí: „Dokonce se uvažuje o tom, že pro nejtěžší zločiny v kyberprostoru by se měl vytvořit mezinárodní tribunál, jenž by byl součástí mezinárodního soudu OSN v Haagu." [46]

V reakcích na kybernetickou hrozbu se objevují nové obranné postupy využitelné i v ochraně obyvatelstva. Např. kanadský fyzik Ben Sussman vyvinul způsob zašifrování elektronické komunikace v ochraně před hackery, který spočívá v generování číselných kódů jako klíče k uzamčení korespondence s citlivými daty. Inspiroval se přitom nezmapovanými zákonitostmi kvantové mechaniky. Obrana spočívá ve vysílání laserových pulzů, trvajících jen miliardtiny vteřiny, proti diamantu, přičemž paprsky vycházející z kamene mají nevypočitatelně odlišnou intenzitu. A právě její měření generuje náhodná čísla. To znemožňuje hackerům vystopovat logiku sestavení číselných klíčů.

Americká vláda myslí boj proti kyberútokům vážně. Vykázala ze země generální konzulku Venezuely v Miami Livii Acostaovou Nogueraovou. Je podezřelá, že se podílela na přípravách kyberútoků proti USA v době, kdy působila na venezuelském velvyslanectví v Mexiku. Podezření je výsledkem prověřování informace španělské televize Univision o účasti Acostaové v debatách o možných kyberútocích proti americké vládě, které vedl Federální úřad pro vyšetřování (FBI). V pořadu pod názvem Íránská hrozba se objevily informace o zapojení kubánské a íránské diplomatické mise v USA na těchto útocích. Acostaová v době působení v Mexiku v roce 2007 údajně chtěla získat informace o serverech jaderných elektráren v USA a dalších citlivých objektech, jakým je Kennedyho letiště v New Yorku. [47]

Podle analýzy společnosti Northrop Grumman pro americký Kongres představují pro USA v případě konfliktu nejvážnější nebezpečí kybernetické schopnosti Číny a její armády Za posledních deset let se operace proti nepřátelským počítačovým sítím staly základním prvkem čínských obranných strategií. Je tomu mj. proto, že má přístup k nejmodernějším technologiím. Na prvém místě je to schopnost narušit pro případ útoku i obrany technologické vybavením protivníka a získávání citlivých údajů z cizích databází. Do tohoto konfliktu mohou být zapojeny i čínské státní telekomunikační firmy. [48]

Je možné ještě doplnit, že i NATO již má svůj **NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)**. Byl otevřen dne 14. 5. 2008 v estonském Tallinu. Členy jsou Estonsko, Lotyšsko, Litva, Německo, Maďarsko, Itálie, Polsko, Slovensko, Španělsko a USA coby přispívající země. My opět na něco potřebného nemáme.

Podobně Evropská unie koncem prvního kvartálu roku 2012 oznámila, že nejspíš od ledna 2013 zřídí v nizozemském Haagu středisko pro boj s kybernetickou kriminalitou s ročním rozpočetem šest milionů euro. Má tu pracovat cca padesát odborníků. [49]

Reakce České republiky

Kybernetickou hrozbu definuje a zabývá se jí Bezpečnostní strategie České republiky 2011 a Bílá kniha o obraně České republiky. Potřebu zajistit bezpečnost toku informací zdůrazňuje i Koncepce pro ochranu obyvatelstva do roku 2013 s výhledem do roku 2020. [50]

Na uvedené bezpečnostní hrozby, zvláště kybernetickou, se zaměřoval Projekt Bezpečnostního výzkumu Ministerstva vnitra Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky.

Ani naše veřejnost nebezpečí kybernetické hrozby nepodceňuje. Odborníci se domnívají, že náš stát musí jasně definovat svou datovou krizovou infrastrukturu. V reálném světě jsou důležité elektrárny, ropovody, nádraží, vodárny, pekárny. Ve virtuálním světě software jaderných elektráren, rozvodných sítí, databází bezpečnostních složek a bankovních serverů jsou důležité především funkční a bezpečné komunikační kanály mezi vládními institucemi. [51]

V Brně vzniklo **Národní centrum kybernetické bezpečnosti.** Má čelit a předcházet internetovým hrozbám a jeho součástí bude vládní koordinační místo pro okamžitou reakci na útoky hackerů. Centrum bude mít za úkol koordinovat činnost státních institucí i veřejného sektoru v případě internetových útoků hackerů. Rozpočet centra na rok 2012 je 50 milionů korun a v dalších letech se bude zvyšovat až nad 60 milionů. Zatím mu ale chybějí jasné kompetence. Nejdříve totiž musí parlament schválit zákon o kybernetické bezpečnosti. [52] Má se tak stát do konce roku 2013. Tento legislativní krok nebude jednoduchý, zasáhne i do práv občanů a firem. V budoucnosti mohou být tímto zařízením bráněny i strategicky důležité firmy a banky. Český internet zatím ochraňuje sdružení cz.nic, které bude spravovat vládní doménu do vybudování vládního střediska. Znamená to, že NBÚ bude plně plnit roli koordinační instituce až po získání příslušných pravomocí. Nyní již však může prověřovat odolnost a bezpečnost rizikových informačních systémů ve státní správě a prověřovat lidi, kteří s nimi pracují.

Na druhé straně podle expertů jednotlivci a soukromé instituce musí nést odpovědnost za zajišťování své bezpečnosti v oblasti informací sami, stát musí příslušně upravit legislativu a zajistit osvětu. Měl by nejspíš také zajistit, aby školy připravovaly absolventy seznámené se zásadami osobní a firemní kybernetické bezpečnosti, protože se jedná o oblast, která postrádá historicky předávané zkušenosti u valné části populace. Zatímco dříve se děti učili od rodičů a prarodičů, v této oblasti je tomu naopak.

Samostatným problémem jsou útoky na kritické infrastruktury, protože ty mohou být jak soukromého, tak státního charakteru, případně kombinací státních a soukromých subjektů. První cílová oblast spadá zcela jednoznačně do působnosti Policie ČR (PČR), a to až do momentu, kdy se útoky stanou natolik masivními a cílenými, že začnou ohrožovat chod státu a začne být zřejmé, že se jedná o hromadný cílený útok, ekvivalentní válce. Jednotlivé útoky je v tomto smyslu třeba pokládat za standardní

přestupky nebo trestné činy, v závislosti na způsobené škodě. Věcí státu je zajistit vyšetřovací policejní jednotky, personálně vybavené kvalifikovanými IT specialisty schopnými tyto útoky a trestné činy vyšetřovat, a to i v zahraničí.

Druhá cílová oblast rovněž spadá podle charakteru útoku také buď do působnosti PČR, popř. BIS. Jedná-li se o útoky na stránky Ministerstva vnitra nebo o pokusy získat informace ze serveru PČR, kdy jde o trestný čin a jeho vyšetřování je v rukou PČR. Jedná-li se o pokus vyřadit z provozu některý operační IS PČR, popř. AČR, může se jednat o teroristický akt, a ten už spadá do působnosti BIS.

Útoky na kritické infrastruktury mají zcela odlišný charakter. Způsobené škody se mohou pohybovat v řádech miliard korun a v jejich důsledku může dojít ke ztrátám na lidských životech. V jejich důsledku může dojít i k výraznému narušení funkcionality státu. Ochrana (tj. zejména prevence) a obrana proti nim spadá nejspíš do působnosti rezortu obrany, který by měl zodpovídat i za koordinaci s PČR při jejich odhalování a likvidaci při koordinaci s BIS. To mj. vyplývá z definice úkolů ozbrojených sil v zákoně o ozbrojených silách. Tyto útoky je nutno řešit jako teroristické činy, bez ohledu na pohnutky a cíle jejich nositelů.

Větší počet útoků vedených na více složek kritické infrastruktury je preventivně nutno považovat za **ekvivalent ozbrojeného útoku** s odpovídajícími organizačními, ekonomickými a zahraničně-politickými kroky. V tomto smyslu je nutné *upravit odpovídající články mezinárodních smluv* včetně např. Washingtonské úmluvy o NATO, **kdy začíná platnost článku 5 pro kybernetický útok a jak má taková pomoc vypadat**.

V České republice je pravděpodobně nejdůležitější bezpečnostní iniciativa v oblasti IT existence a aktivity CERT a CSIRT týmů národního týmu CSIRT.CZ, který vznikl v roce 2007 jako národní CSIRT tým v roce 2010.

Závěr

I když nejsou jednotné názory na vážnost kybernetické hrozby a možnost rozsáhlejší kyberválky, převažuje varovné mínění, které není možné podceňovat. Jde o velmi sofistikovaný útočný nástroj, proti němuž není jednoduchá obrana. [53] Navíc je několikanásobně nákladnější. Již nyní jde řádově o desetitisíce případů a škody v řádu miliard. Netýkají se jenom vládních institucí, ozbrojených složek, ale i ekonomických organizací a následně či přímo jednotlivců. Vážným problémem je, že aktéry jsou dosud převážně nevyzpytatelní hackeři, u nichž není možné predikovat jejich aktivity. Daleko vážnější však bude, jakmile se aktéry stanou státy, jak se to prokázalo v případě útoku na estonské sítě a íránský jaderný potenciál. Ale opět to může být v některých případech přijatelnější varianta než vojenský útok s klasickými zbraněmi nebo dokonce zbraněmi hromadného ničení.

Novým jevem je fakt, že bezpečnostní kybernetická hrozba nemá přesnou adresu původce a potenciálního útočníka. Státní hranice a vojenské strategie o prostoru a čase v dosavadní konzervativní podobě se stávají bezvýznamnými.

Z vojenského hlediska je zřejmé, že kybernetické útoky a obrana proti nim jsou a budou součástí ozbrojených aktivit. Je tomu tak proto, že vojáci považují internet a virtuální prostor vůbec jako další, pátou oblast nasazení sil, vedle země, vzduchu, vody a vesmíru. Společenství členských zemí Severoatlantické aliance, které je totálně závislé na elektronické komunikaci je proto extrémně zranitelné. Projevilo se to již v kosovském

konfliktu. Kybernetické vedení války je zákeřné zvláště na počátku pro svou asymetričnost, tj. malou schopnost identifikovat rychle útočníka a nízké náklady, což je výhodou pro útočníka. Proto si armády začínají vytvářet i zvlášť určené jednotky. Stát zabezpečuje příslušný právní a politický prostor, jak je tomu v případě směrnice amerického prezidenta k boji proti kybernetickým útokům. U nás, včetně armády, jsou tyto aktivity zatím na samotném počátku.

Je patrné, že Čína, Rusko a další východní země obecně kromě přípravy na potenciální kybernetické konflikty a obranu proti nim preferují ovládnout on-line prostředí a zamezit šíření informací, západní země zdůrazňují ochranu lidských práv duševního vlastnictví a kybernetickou bezpečnost.

Autor děkuje za podnětné návrhy Vladimírovi Bäumelovi, Felixovi Černochovi, Jaromírovi Novotnému, Bohuslavovi Pernicovi, Jaroslavovi Štefcovi a Štefanovi Volnerovi.

Poznámky k textu a literatura:

[1] RAŠEK, A. Bezpečnostní předpoklady a hrozby: Ekonomická, religiózní a kybernetická bezpečnostní rizika. *Vojenské rozhledy,* 2011, roč. 20, č. 2, s. 38-52, ISSN 1210-3292. **Černá labuť** je označení závažné události retrospektivně předvídatelné (nikoli avšak prospektivně), N.N. Taleb, Černá labuť, Paseka, 2011, ISBN: 978-80-7432-128-3, 478 str. Termín **divoká karta** má původ v karetních hrách, postupně se však rozšířil do dalších oblastí. Je to málo pravděpodobná událost s významnými důsledky (Wikipedie).

[2] Podle pracovního textu Vladimíra Bäumela.

[3] Podle vyjádření Jaroslava Štefce k pracovní verzi tohoto textu.

[4] *Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu.* Praha: Ministerstvo vnitra České republiky, odbor bezpečnostní politiky, 2004.

[5] Z pracovního textu Štefana Volnera.

[6] Dostupné na *http://zpravy.ihned.cz/c1-51699050-valka-na-ctvrt-hodiny.*

[7] Asociace pro mezinárodní otázky, ČR. *Confronting Cyberterrorism: Tackling Political Aspects of Cybersecurity.*

[8] Experti ČVUT spolupracují od roku 1999 s Američany na kybernetické bezpečnosti letecké a námořní dopravy.

[9] Dostupné na *http://www.rozhlas.cz/zpravy/blizkyvychod/_zprava/iran-tvrdi-ze-sestrelil-americke-bezpilotni-letadlo-985595.*

[10] Dostupné na *http://www.itbiz.cz/clanky/bezpecnostni-prehled-stuxnet-2-0-kadafimu-hrozila-i-kybervalka-a-vyvoj-androidu-se-zabezpecenym-jadrem.*

[11] **Malware** je počítačový program určený ke vniknutí nebo poškození počítačového systému. Výraz malware vznikl složením anglických slov „malicious" (zákeřný) a „software" a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware (Wikipedie).

[12] Dostupné na *http://www.itbiz.cz/clanky/bezpecnostni-prehled-stuxnet-2-0-kadafimu-hrozila-i-kybervalka-a-vyvoj-androidu-se-zabezpecenym-jadrem.*

[13] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/249016-dva-satelity-nasa-ovladli-hackeri-mohli-je-nechat-spadnout.html.*

[14] Dostupné na *http://zpravy.ihned.cz/svet-blizky-vychod/c1-46784300-kybervalka-v-plnem-proudu-iran-hlasi-zadrzene-spiony-evropa-zbroji.*

[15] *CNN*, 14. 11. 2011.

[16] Dostupné na *http://paggio.blog.idnes.cz/c/175654/Kybervalka-hudba-budoucnosti.html.*

[17] Dostupné na *http://www.itbiz.cz/clanky/bezpecnostni-prehled-stuxnet-2-0-kadafimu-hrozila-i-kybervalka-a-vyvoj-androidu-se-zabezpecenym-jadrem;* respektive;h*ttp://technet.idnes.cz/byl-odhalen-nejvetsi-cyber-utok-v-historii-virus-flame-radil-pet-let-v-iran-a-izrael-gei-/sw_internet.aspx?c=A120528_143110_sw_internet_vse.*

[18] Studii *In the Dark: Crucial Industries Confront Cyberattack*s [V temnotě: Klíčová infrastruktura vs. kybernetické útoky] vypracovala na objednávku společnosti McAfee organizace CSIS. „Zjistili jsme,

že přijetí bezpečnostních opatření v civilním průmyslu nestačí držet krok s nárůstem hrozeb, k němuž došlo za poslední rok," uvedl Stewart Baker, který řídil studii na straně CSIS. Zavádění nových bezpečnostních technologií je podle Barkera pomalé. Specialisté na zabezpečení IT jsou se svými názory téměř osamoceni. 90-95 % lidí pracujících ve firmách provozujících rozvodné sítě nemá z nedostatečného zabezpečení obavy a bezpečnost IT systémů vnímají až na posledním místě v seznamu věcí, které je třeba kontrolovat. Provoz současné kritické infrastruktury je přitom na fungování řídicích počítačových systémů ve velké míře závislý. Tyto systémy se nejčastěji označují jako SCADA (supervisory control and data acquisitions, doslova „nadřazené řízení a sběr dat"). Kromě zranitelností samotných systémů je dalším problémem mnohdy nevhodný návrh sítí. Často fungují tak, že i relativně drobné narušení se může kaskádovitě šířit, a nakonec vyřadit z provozu značnou část sítě (např. při výpadcích dodávek proudu – tzv. blackout).Dostupné na *http://securityworld.cz/securityworld/in-the-dark-roste-pocet-utoku-proti-kriticke-infrastrukture-3545.*

[19] „Několikrát ročně, zhruba každé dva až tři měsíce, zaznamenáme delší výpadek v řádu několika desítek minut, který je způsoben různými technickými problémy na straně bankovních systémů. Ihned informujeme přes web klienty. Drobnější problémy v řádu minut bývají také způsobeny například výpadky při zasílání autorizačních SMS ze strany mobilních operátorů," potvrdil Právu Jakub Puchalský z Raiffeisenbank. Kromě toho jsou systémy jednou za měsíc plánovaně odstaveny. „Klienti jsou vždy dopředu o této skutečnosti informováni," zdůraznil Puchalský. Právě to, že se někdy lidé o selhání systémů nemusejí dozvědět nejdříve od banky, ale až když jsou vystaveni značnému překvapení, bývá hlavním důvodem stížností a rozčarování, tak jak se to stalo v nedávném případě nevratné ztráty části dat u odchozích plateb několika klientů ČSOB. Dostupné na *http://www.novinky.cz/finance/250899-kolapsum-v-internetovem-bankovnictvi-banky-neumeji-zabranit.html?ref=stalo-se.*

[20] Obama se obává, že americké telefonní sítě „volají" samy do Číny. *MF DNES,* 2. 12. 2011, s. 8A.

[21] Dostupné na *http://paggio.blog.idnes.cz/c/175654/Kybervalka-hudba-budoucnosti.html.*

[22] Dostupné na *http://www.novinky.cz/finance/250899-kolapsum-v-internetovem-bankovnictvi-banky-neumeji-zabranit.html?ref=stalo-se.*

[23] Dostupné na *http://zpravy.ihned.cz/c1-51699050-valka-na-ctvrt-hodiny.*

[24] Tamtéž.

[25] Dostupné na *http://www.novinky.cz/internet-a-pc/254481-hackeri-napadli-americkou-poradenskou-firmu-chteji-ukrast-milion-a-rozdat-jej.html?ref=zpravy-dne.*

[26] Dostupné na *http://aktualne.centrum.cz/zahranici/blizky-vychod/clanek.phtml?id=727408.*

[27] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/255356-pocitacovym-hrozbam-kraluji-viry-sirici-se-pres-usb-flash-disky.html.*

[28] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/255707-hackeri-na-internetu-zverejnili-e-maily-a-hesla-lidi-z-nato.html?ref=stalo-se.*

[29] Dostupné na http://www.tyden.cz/rubriky/media/pocitace/internetove-bankovnictvi-ohrozuje-virus-u-mi-zamest-stopy_221993.html.

[30] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/255595-nebezpecny-pocitacovy-virus-vykrada-lidem-bankovni-ucty.html?ref=boxE.*

[31] Dostupné na *www.itbiz.cz/zpravicky/jake-kyberneticke-hrozby-nas-cekaji-v-roce-2012.*

[32] Dostupné na *www.techmagazin.cz/447.*

[33] Dostupné na *www.novinky.cz/internet-a-pc/bezpecnost/255722-pocitacovi-podvodnici…*

[34] Menším písmem uvedené příklady jsou čerpány s tohoto zdroje. Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/255722-pocitacovi-podvodnici-zkouseji-na-duverive-uzivatele-nove-triky.html?ref=ostatni-clanky.*

[35] Tokio má kyberzbraň na hackery, *Právo,* 3. 1. 2012.

[36] Systematická příprava Číny na kybernetickou válku je notoricky známa, mj. na *http://is.muni.cz/th/342895/fss_m/Budoucnost.kyber.teror.Aberle.DP.pdf.*

[37] Dostupné na *http:// jedenbod.cz/.*

[38] BECK, Ulrich. *Riziková společnost: na cestě k jiné moderně.* Vyd. 1. Praha: Sociologické nakladatelství, 2004. 431 s. ISBN 8086429326.

[39] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/248924-hacker-ktery-nakazil-zakernym-virem-12-milionu-pocitacu-skoncil-v-poutech.html.*

[40] Novinky.cz 1. 6. 2011. Dostupné na *http://www.novinky.cz/zahranicni/amerika/235023-kyberneticky-utok-muze-podle-usa-vyvolat-vojenskou-odvetu.html?ref=stalo-se* Dostupné na *http://aktualne.centrum.cz/zahranici/amerika/clanek.phtml?id=702234.*

[41] Dostupné na *http://zpravy.ihned.cz/svet/c1-52146300-obama-podepsal-nova-pravidla-pro-vedeni-kybernetickych-valek.*

[42] Dostupné na *http://paggio.blog.idnes.cz/c/175654/Kybervalka-hudba-budoucnosti.html.*
[43] Dostupné na *http://zpravy.ihned.cz/svet-blizky-vychod/c1-46784300-kybervalka-v-plnem-proudu-iran-hlasi-zadrzene-spiony-evropa-zbroji. www.nato.int/docu/review/2011/11-september/Cyber-Threads/CS/index.htm.*
[44] Zdroj: HelpNet Security. Dostupné na *http://byznys.lidovky.cz/kybervalka-neni-vymysl-tvrdi-vyvojar-antiviru-frx-/firmy-trhy.asp?c=A111113_095835_ln_domov_spa.*
[45] Dostupné na *http://zpravy.ihned.cz/c1-51699050-valka-na-ctvrt-hodiny.*
[46] Tamtéž.
[47] Dostupné na *http://aktualne.centrum.cz/zahranici/amerika/clanek.phtml?id=728041.*
[48] Dostupné na *http://www.novinky.cz/internet-a-pc/bezpecnost/261313-kyberneticke-schopnosti-ciny-predstavuji-pro-americany-opravdove-nebezpeci.html. www.earchiv.cz/b11/b1107001.php3.*
[49] *ČTK,* 27. 3. 2012.
[50] Zatímco v jiných zemích – jako příklad by bylo možné uvést Spojené státy – se obvykle se strategickými a koncepčními dokumenty odpovědně pracuje a podle nich také jedná, nedá se to říci o podobných materiálech našich. Příkladem může být např. uvedená Bezpečnostní strategie ČR, jejíž kvalita zpracování sice byla nesporně lepší než v minulosti, ale přesto po jejím schválení se o tom v podstatě nedozvěděla veřejnost, stejně tak ji přešla většina médií mlčením. Je to jistě záležitostí relevantních orgánů a institucí, které za tvorbu a realizaci příslušných strategických dokumentů a jejich realizaci odpovídají. Ale možná je to i v samotných dokumentech, která by měly svým obsahem a závaznými závěry tomu předejít. Nesporně by se proto mělo pracovat i na metodice tvorby těchto dokumentů, která by měla nejen pomoci zlepšit kvalitu jejich tvorby, ale i obecnou informovanost o nich, a zejména zajistit jejich realizaci.
[51] Dostupné na *http://paggio.blog.idnes.cz/c/175654/Kybervalka-hudba-budoucnosti.html.*
[52] Dostupné na *http://www.rozhlas.cz/brno/zpravodajstvi/_zprava/966648.*
[53] Kategorie resp. termín **obrana** se stále výrazněji ocitá v nejednoduché interpretační situaci, a to zvláště v nejobecnějším slova smyslu, např. při tvorbě dokumentu o strategii obrany České republiky. Je historicky spojen s komplikovanými konotacemi. Obranou obecně rozumíme schopnost odvrátit útok, ohrožení, nástrahy, nebezpečí ap. Obrana obvykle znamenala bránit se před někým a něčím, v geopolitickém slova smyslu především před sousedy. I když s technologickým vývojem, např. letectva, raketového vojska, ale i kybernetiky a internetu, také tato hranice padá. Rozpaky přesto zůstávají, a to zejména proto, že se sousedy jsme v dobrých vztazích, stejně tak jsme s nimi a ostatními členy seskupení států, jako je Evropská unie a Severoatlantická aliance. Tudíž jsme před nutností se s tímto pojmem vyrovnat. Pracovně se nabízí využít příslovce „spolu“ jako první části složených slov spojujících část druhou s významem příslovce spolu, společně, a to jako bližší okolnosti jejího děje nebo vlastnosti. Jde tedy o slovo, resp. novotvar **spoluobrana**. Podobných složených slov s příslovcem *spolu-* má spisovná čeština ke dvěma stovkám (spoluautor, spolucestující, spolujezdec, spoluobčan, spolupachatel, spolupracovník, spoluzakladatel, spolužák apod.) a tvoří se další. Některé složeniny mají blízko i k vojenství (spolubojovník i dokonce spoluvelitel). Nejde ale jen o nalezení pojmu lépe vystihujícího obsah konkrétní měnící se aktivity, adekvátní slovo nebo novotvar zároveň nutí i jinak jednat, v konkrétním případě slova spoluobrana, resp. nalezení slova adekvátněji vystihujícího obsah, nutí myslet, tvořit a chovat se účelněji, v daném případě globálně, transatlanticky, evropsky, a samozřejmě jednat lokálně s vědomím sounáležitosti s existujícími seskupeními, jejichž jsme členy, respektovat jejich funkce, záměry a cíle, které také ovlivňovat v souladu se zájmy národními. Pojem *spoluobrana* je tedy v jistém smyslu mezi *národní* a *kolektivní obranou,* resp. dále individuální obranou.

Politicko-vojenské ambice pro výstavbu ozbrojených sil České republiky jsou politickým zadáním pro ozbrojené síly České republiky k jejich rozvoji a zajištění závazných povinností, spojeneckých závazků a případně dalších úkolů. Rozvoj vojenských schopností ozbrojených sil České republiky respektuje závěry Bílé knihy o obraně z roku 2011 a je určován kvalitativními a kvantitativními kritérii.

Z Obranné strategie České republiky, chváleno vládou ČR 26. 9. 2012.