POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Kybernetická válka

Diplomová práce

Cyber War
Master Thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Bc. Václav NOVÁK

PRAHA
2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 15. 3. 2023

Bc. Václav NOVÁK

Poděkování

Děkuji tímto vedoucímu mé diplomové práce, RNDr. Václavu Hníkovi CSc., za konzultace, cenné rady a připomínky.

ANOTACE

Diplomová práce se zabývá problematikou kybernetických válek a s tím související kybernetické bezpečnosti. V rámci teoretické části jsou úvodem vymezeny základní pojmy, které se v práci vyskytují a jejichž vymezení je z hlediska zkoumané problematiky nezbytné. Prostor je dále věnován vývoji bezpečnostní situace ve 21. století a technologického pokroku. Analytická část práce se zabývá případovou studií konfliktu mezi Spojenými státy a Íránem. Úvodem této části práce je zkoumaný incident zasezen do souvislosti s íránským jaderným programem a následně podrobněji popsán z několika perspektiv.

KLÍČOVÁ SLOVA

kybernetická válka * kybernetická bezpečnost * kybernetický útok * kybernetický prostor * bezpečnostní situace * Spojené státy * Írán * íránský jaderný program

ANNOTATION

The master thesis deals with the issue of cyber wars and related cyber security. In the framework of the theoretical part, the basic concepts that occur in the work and whose definition is necessary from the point of view of the researched issue are defined in the introduction. The space is also devoted to the development of the security situation in the 21. century and technological progress. The analytical part of the work deals with a case study of the conflict between the United States and Iran. At the beginning of this part of the work, the investigated incident is placed in the context of the Iranian nuclear program and then described in more detail from several perspectives.

KEYWORDS

cyber war * cyber security * cyber attack * cyberspace * security sutiation * United States * Iran * Iranian nuclear program

Obsah

Úvod 7
I. TEORETICKÁ ČÁST 9
1. Vymezení základních pojmů 9
1.1 Tradiční válka a hybridní válka 9
1.2 Informační válka 10
1.3 Kybernetická válka a síťová válka 11
1.4 Kybernetický útok 12
1.5 Kybernetické hrozby 15
1.6 Kybernetický prostor 17
1.7 Kybernetická bezpečnost a obrana 18
1.8 Shrnutí 21
2. Bezpečnostní situace 21. století 22
2.1 Kyberprostor jako specifická oblast bezpečnosti 23
2.2 Informační revoluce 25
2.3 Revoluce ve vojenských záležitostech 27
2.4 Shrnutí 29
II. ANALYTICKÁ ČÁST 31
3. Konflikt Spojené státy-Írán 31
3.1 Počátek konfliktu 32
3.2 Stuxnet 37
3.3 Reakce Íránu na nasazení Stuxnetu 41
3.3.1 Operace Newcaster 41
3.3.2 Operace Cleaver 43
3.3.3 Shamoon 45

3.3.4 Operace Ababil 46
3.3.5 Další aktivity íránských hackerů 46
3.4 Spojené státy a kyberprostor 48
3.5 Irán a kyberprostor 49
Závěr 55
Seznam použité literatury 58

Úvod

Snad je na světě jen minimum těch, v nichž by slovo „válka“ evokovalo cokoli příjemného. Přesto je toto téma přímo či nepřímo obsahem většiny zpravodajských relací a odborných diskusí jak na národní, tak i mezinárodní úrovni, a v důsledku toho se stále častěji promítá i do uvažování většiny obyčejných lidí. Dne 24. 1. 2023 se tzv. hodiny posledního soudu posunuly nejblíže k půlnoci v historii měření (90 sekund před půlnocí), především kvůli probíhající válce na Ukrajině a téměř pravidelnému vyhrožování jaderným útokem především ze strany Ruska[1]. Vedle toho se stále častěji hovoří také o zvyšujícím se riziku ozbrojeného střetu mezi Spojenými státy a Čínou, a rovněž je nutné brát v potaz i další skutečnosti, jakými jsou ekonomické hrozby na pozadí těchto sporů či rozpory v nadnárodních organizacích typu Evropské unie nebo NATO. Nelze si přitom nevšimnout jistých paralel s obdobími předcházejícími předešlým světovým konfliktům, a ačkoli autor zůstává v této otázce opatrným optimistou, považuje za nezbytné věnovat studiu problematiky pozornost. To se týká také kybernetické války coby jednoho z nekonvenčních nástrojů vedení boje. Význam kybernetického prostoru neustále narůstá spolu s tím, jak roste míra naší závislosti (a rovněž také zranitelnosti) na moderních technologiích. To si uvědomují i jednotlivé státy, které na působení v kybernetickém prostoru vynakládají svůj finanční i intelektuální kapitál ve snaze zaujmout dominantní postavení podobně, jako tomu je v rámci konvenčního prostředí.

Diplomová práce se proto snaží přiblížit problematiku kybernetických válek a s tím související kybernetické bezpečnosti v kontextu mezinárodní bezpečnostní situace odpovídající podmínkám na počátku 21. století. Předmětem zkoumání je konflikt mezi Spojenými státy a Íránem ohledně íránského jaderného programu vymykajícímu se mezinárodnímu dohledu, z hlediska kybernetických aktivit obou jmenovaných aktérů. Cílem práce je

[1] viz MECKLIN, John. A time of unprecedented danger: It is 90 seconds to midnight. *Bulletin of the Atomic Scientists* [online]. 2023. [cit. 12.2.2023]. Dostupné z: https://thebulletin.org/doomsday-clock/current-time/

ověření hypotézy, že mezi Spojenými státy a Íránem probíhá plnohodnotná kybernetická válka.

Práce je členěna na dvě části, část teoretickou a část analytickou. V rámci teoretické části jsou úvodem vymezeny základní pojmy, které se v práci vyskytují a jejichž definice je z hlediska zkoumané problematiky nezbytná. Prostor je dále věnován vývoji bezpečnostní situace ve 21. století pohledem z několika perspektiv – pohledem obecného technologického pokroku, reakce teorie mezinárodních vztahů na tento pokrok, a rovněž tak perspektivou vojenskou. Analytická část práce se zabývá případovou studií konfliktu mezi Spojenými státy a Íránem. Úvodem této části je zkoumaný incident zasezen do souvislosti s íránským jaderným programem a následně podrobněji popsán z několika perspektiv, přičemž důraz je kladen především na aktivity odehrávající se v kybernetickém prostoru. Zvláštní důraz je přitom vždy věnován motivaci útočníků a důkazům či výpovědím zainteresovaných jedinců hovořících o vazbách útočníků na zkoumané státní aktéry.

Případová studie se opírá především o informace z odborné, převážně cizojazyčné literatury, webových stránek zainteresovaných institucí, zpráv publikovaných organizacemi zabývajícími se kybernetickou či mezinárodní bezpečností, a dále pak čerpá z článků zahraničních zpravodajských serverů dokumentujících jednotlivé kybernetické útoky.

Překážkou při zpracování případové studie byla poměrně značná absence oficiálních íránských stanovisek nebo důležitých dat. Příčinou může být jednak samotná jazyková bariéra, jednak značná disproporce v objemu amerických (či šířeji západních) a íránských materiálů.

I. TEORETICKÁ ČÁST

1. Vymezení základních pojmů

Studium kybernetických válek a s tím neodmyslitelně související kybernetické bezpečnosti je multioborovou disciplínou přesahující jak do technických, tak i netechnických oborů. Lze se při něm setkat s řadou slovních spojení a termínů, které mohou být vzájemně zaměňovány či interpretovány různými způsoby. Proto je vhodné v rámci následující kapitoly vymezit základní pojmy, které jsou podstatné pro pochopení této problematiky.

1.1 Tradiční válka a hybridní válka

Válka sama o sobě je poměrně široký pojem, neboť prochází historickým vývojem stejně jako její teoretické zkoumání, a lze ji tak nahlížet z mnoha perspektiv – z vojenské, politické, psychologické apod. Pro účely této práce nicméně postačí obecná definice války převzatá z díla autorů McCulloha a Johansona, kteří válku považují za *„organizovaný konflikt mezi ozbrojenými sáty, národy nebo jinými stranami v určitém období, k dosažení požadovaného politického/ideologického cílového stavu“*[2].

Hybridní válka (někdy též nazývaná alternativní či nelineární válkou) je širším pojmem a je možno ji chápat jako vedení konfliktu za využití kombinace konvenčních i nekonvenčních prostředků, působících ve vzájemné synergii a zahrnujících širokou škálu nástrojů, mimo jiné například ekonomické nástroje, psychologické operace, kybernetické útoky nebo prvky informační války popsané dále[3]. Cílem hybridní války je subverze (podvratná činnost), kterou Kříž[4] člení do čtyř etap:

- demoralizace cílové společnosti,

[2] viz s. 182, McCULLOH, Timothy B. a Richard B. JOHNSON. *Hybrid Warfare*. Florida: MacDill Air Force Base, 2013. ISBN 978-1-933749-77-8.
[3] tamtéž.
[4] viz s. 11, KŘÍŽ, Zdeněk et al. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. Ostrava: Jagello, 2015. ISBN 978-80-904850-2-0.

- destabilizace této společnosti,
- následné vyvolání krize,
- převzetí kontroly nad cílovou společností vnitřními silami napojenými na útočníka.

Kříž[5] dále uvádí, že jde o starý sovětský koncept, který uplatňoval SSSR po celou dobu své existence vůči západním zemím, nicméně některé její prvky a fáze popsané výše lze nepochybně pozorovat například i v současném konfliktu Ruska s Ukrajinou, a to zřejmě na obou stranách.

1.2 Informační válka

Zřejmě proto, že prostředky kybernetické války jsou informační technologie, bývá v některých případech zaměňován pojem kybernetická válka s termínem informační válka. Takový přístup není správný, neboť informační válka je pojmem širším a zahrnuje řadu dalších, vzájemně se prolínajících a doplňujících operací, mezi něž patří působení na velení a řízení, zpravodajské působení, psychologická a diplomatická válka a řada dalších, včetně právě kybernetické války.[6]

Označení „válka“ v tomto kontextu může evokovat dojem čehosi vzdáleného, Evropě (alespoň té západní) se vyhýbajícího, nicméně například v roce 2016 vydalo BIS zprávu, dle které vedlo o rok dříve Rusko informační válku v České republice v souvislosti s ukrajinským a syrským konfliktem.[7] Informační válka je tedy relativně běžným jevem, což ale na jejím významu a hrozbách nikterak neubírá.

---

[5] viz s. 11, KŘÍŽ, Zdeněk et al. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. Ostrava: Jagello, 2015. ISBN 978-80-904850-2-0.
[6] viz KUBEŠA, Milan. Vojenské klamání v informačním věku. *Vojenské rozhledy* [online]. 2013, roč. 22 (54), č. 1. [cit. 17.10.2022]. ISSN 2010-3292. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/vojenske-klamani-v-informacnim-veku
[7] viz ČESKÁ TELEVIZE. Ruští špioni vedou v ČR informační válku, činští usilují o vliv, říká zpráva tajné služby. *Česká televize* [online]. 2016. [cit. 14.11.2022]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/1893620-v-cesku-loni-nejvice-pusobili-spioni-z-ruska-a-ciny

1.3 Kybernetická válka a síťová válka

Kybernetická válka je relativně nový fenomén, který se do popředí zájmu dostává teprve v posledních několika dekádách, přesto se lze setkat s celou škálou definic.

Výkladový slovník kybernetické bezpečnosti ji definuje jako *„použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků“*[8]. Z dalších definic lze zmínit státocentrické pojetí Clarka a Knakea: *„jakékoli jednání státu za účelem způsobení škody prostřednictvím infiltrace do počítačů či počítačových sítí jiného státu“*[9], kteří zřetelně kladou důraz na státní aktéry; nebo naopak Cornishovo pojetí hovořící o konfliktu *„nejenom mezi státy, ale může zahrnovat i nestátní subjekty. V kybernetické válce je obtížné přesně zacílit s přiměřenou silou; cílem mohou být vojenské, průmyslové nebo civilní objekty, nebo to může být server, který hostí širokou škálu klientů, mezi nimiž je pouze jeden zamýšlený cíl“*[10].

Přestože výše uvedený výčet definic není komplexní, zřetelně ilustruje rozdíly v pojetí jednotlivých autorů. Dvě posledně jmenované definice si na první pohled odporují ve vymezení subjektů zahrnovaných do konfliktu. V případě pojetí Jiráska a kol., je zase nutné klást otázku (v souladu s Clarkem a Knakeem), zda kybernetickou válkou nemůžeme označit i hypotetický asymetrický konflikt mezi dominantním útočníkem a slabším cílem, neschopným obrany, ačkoli, přísně vzato, takovou interakci by zřejmě bylo příhodnější považovat za soubor kybernetických útoků.

Síťová válka je koncept, který byl představen počátkem 90. let minulého století společností RAND Corporation, financovanou vládou Spojených států. Autoři pod hlavičkou této organizace Arquilla a Ronfeldt jí chápou jako konflikt

---

[8] viz s. 58, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[9] viz s. 11, CLARKE, Richard A. a Robert K. KNAKE. *The Next Threat to National Security and What to Do About IT*. New York: HarperCollins, 2010. ISBN 978-0-06-199239-1.

[10] viz s. 37, CORNISH, Paul et al. *On Cyber Warfare*. London: The Royal Institute of International Affairs, 2010. ISBN 978-1-86203-243-9.

mezi národy nebo společnostmi, jehož cílem je ovlivnit mínění cílové populace, přičemž aktéry na straně útočníků mohou být jednak státy samotné, častěji ale státem podporované či samostatně působící skupiny, včetně teroristických či zločineckých organizací. Je to tedy určitý druh války, který je spojen s informacemi a znalostmi společnosti, a může mít podobu propagandy, politických podvratných činností, zviditelnění opozice apod.[11]

1.4 Kybernetický útok

Samotný kybernetický útok je možno vymezit podle slovníku kybernetické bezpečnosti jako *„útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či strategicky motivovaných útoků“*[12]. Zdánlivě podobné, přesto významově užší pojetí nabízí Tallinský manuál 2.0, který jej definuje slovy *„kybernetický útok je kybernetická operace, ať už útočná nebo obranná, u které lze důvodně očekávat, že způsobí zranění nebo smrt osob nebo poškození či zničení majetku“*[13].

Zmíněný rozdíl u posledně jmenované definice spočívá především v předpokladu schopnosti působit prostřednictvím tohoto typu útoku škodu na majetku či dokonce zdraví lidí, zatímco otázku špionáže ponechává stranou zájmu. Především v anglosaském prostředí se pak lze setkat s rozdělením na tzv. computer network attack (CNA), kterým je myšlen ničivý kybernetický útok, a computer network exploitation (CNE), jenž lze chápat jako neničivý útok špionážního charakteru.[14]

---

[11] viz s. 28, ARQUILLA, John a David RONFELDT. Cyberwar is Coming! *Rand Corporation* [online]. 1993. [cit. 15.10.2022]. Dostupné z: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

[12] viz s. 59, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[13] viz s. 415, SCHMITT, Michael N. *Tallin Manual 2.0: On the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, 2017. ISBN 978-1-107-17722-2.

[14] viz s. 2, OWENS, William A., DAM, Kenneth W. a LIN, Herbert S. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. *National Academies* [online]. 1993. [cit. 18.10.2022]. Dostupné z: https://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf

Kybernetické útoky lze členit do dvou základních kategorií – na plošné a cílené:

- Plošné útoky, které bývají relativně méně sofistikované a jsou proto realizovány mnohem častěji. Využívají se zejména v oblasti kybernetické kriminality. Šulc uvádí, že při tomto typu útoku *„útočník hledá nejjednodušší, nerychlejší a nejlacinější způsob, jak do daného systému proniknout, kompromitovat ho a poté využít. Pokud útočník hned napoprvé neuspěje, jde dál a nezdržuje se, chová se totiž naprosto racionálně, neboť ví, že brzy jistě narazí na jiný systém, který bezpečnost absolutně neřeší a do které bude snadné proniknout“*[15]. Z uvedeného vyplývá možnost bránit se těmto typům útoků běžným zabezpečením systému.
- Cílené útoky a APT (Advanced Persistent Threat). Jak implikuje samotné označení, jedná se o útok na konkrétní cíl (organizaci, příp. osobu), přičemž útočníkem bývá obvykle státní aktér, příp. státem podporovaná organizace, neboť tento typ je zpravidla technologicky, finančně i časově náročný a využívá širokou škálu pokročilých technik a prostředků.[16] Lze rozlišovat jednorázové útoky a tzv. Advanced Persistent Threat (dále jen APT), jejichž účelem je *„dlouhodobé a vytrvalé infiltrování a zneužívání cílového systému za pomoci pokročilých a adaptivních technik“*[17].

Jestliže byly v předchozím odstavci zmíněny prostředky kybernetických útoků, je na místě tyto nástroje alespoň stručně přiblížit, přičemž pozornost je věnována zejména těm nejčastěji využívaným:

- Malware, termín, který vznikl složením anglických slov „malicious“ a „software“, označuje jakýkoli software určený k narušení standardních činností počítačového systému, zisku informací nebo k získání přístupu k počítačovému systému.[18] Může cílit na konkrétní subjekt nebo mít

[15] viz s. 32, ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
[16] viz s. 37, ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
[17] viz s. 74, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
[18] viz s. 204, KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

i plošný charakter.[19] Jirovský rozlišuje malware dle způsobu šíření na červy (program, který dokáže sám sebe kopírovat a následně sám sebe šířit po síti nebo se rozesílat prostřednictvím emailových adres), trojské koně (vydává se za nějakou aplikaci či její aktualizaci, oběť si jej sama stáhne) a viry (kopíruje a vkládá sám sebe do cílového souboru, po jehož spuštění se snaží infikovat další soubory); příp. dle projevu na reklamní malware, zadní vrátka, bankovní malware a logickou bombu.[20]

- Ransomware, který je schopný zašifrovat data na koncovém zařízení a jejich zpřístupnění umožní až po zaplacení výkupného, může mít podobu například viru či trojského koně.[21]
- Spyware, tedy špionážní software, jehož úkolem je odesílat data a informace o uživateli infikovaného zařízení subjektu, který program vytvořil nebo distribuoval.[22]
- Botnet, ten lze chápat jako síť infikovaných zařízení kontrolovanou útočníkem (či skupinou útočníků), např. za účelem rozesílání spamových emailů, podvodným zapojováním těchto zařízení do kampaní či pro tzv. DDoS útoky.[23]
- DDoS (Distributed Denial of Service) útoky, jejichž hlavním cílem je tzv. „odepření služby“. Toho lze dosáhnout tak, že útočník zahltí cílový systém velkým množstvím požadovaných úloh,[24] jedná se tedy o formu cílených útoků.

---

[19] viz s. 45,ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
[20] viz JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Granda, 2007. ISBN 978-80-247-1561-2.
[21] viz s. 83, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
[22] viz s. 96, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
[23] viz LUTKEVICH, Ben. What is Botnet? *Techtarget* [online]. 2021. [cit. 29.10.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/botnet
[24] viz s. 35, ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

1.5 Kybernetické hrozby

Hrozbu lze v obecné rovině chápat jako *„potenciální příčinu nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace“*[25]*.* V prostředí kyberprostoru je problematika konceptualizace pojmu hrozba obzvláště náročná. Hrozbou může být jak neintencionální chyba, které se programátor dopustí při vývoji určitého softwaru, a která tak vytváří potenciální ohrožení subjektu využívajícího daný software, tak i intencionální cílené vyhledávání nedostatků příslušného softwaru se záměrem těchto nedostatků využít k poškození cílového subjektu. Lze se proto setkat s řadou definic kybernetických hrozeb, některé z nich neintencionální chyby postihují, jiné nikoli. Americká CISA (Cybersecurity & Infrastructure Security Agency) definuje kybernetickou hrozbu následovně: *„Kybernetická hrozba odkazuje k osobám snažícím se o neautorizovaný přístup k zařízení kontrolního systému a/nebo síti používající dráhy datové komunikace. Tento přístup může být řízen zevnitř organizace důvěryhodnými uživateli nebo ze vzdálených míst neznámými osobami používajícími internet. Hrozby mohou přicházet z mnoha směrů, včetně nepřátelských vlád, teroristických skupin a jiných škodlivých vetřelců“*[26]*.*

Shackelford rozlišuje kybernetické hrozby dle motivu a prostředků útočníka do čtyř hlavních skupin[27]:

- Kybernetická špionáž, prováděná za účelem odhalení citlivých vládních informací, obchodních tajemství či jakýchkoli jiných informací za účelem dosažení zisku nebo získání moci (potažmo výhody) s minimálními náklady. Cornish považuje špionážní akce za nejčastěji prováděné nelegální aktivity v kyberprostoru.[28] Výkladový slovník kybernetické bezpečnosti předkládá státocentrickou definici kybernetické špionáže,

[25] viz s. 42, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
[26] viz DEPARTMENT OF HOMELAND SECURITY. Cyber Threat Source Descriptions. *CISA* [online]. 2005. [cit. 15.11.2022]. Dostupné z: https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions
[27] viz SHACKELFORD, Scott J. Towards Cyber Peace: Managing Cyber Attacks Through Polycentric Governance. *American University Law Review* [online]. 2013, roč. 62, č. 5. [cit. 17.11.2022]. Dostupné z: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1888&context=aulr
[28] viz s. 8, CORNISH, Paul et al. *On Cyber Warfare*. London: The Royal Institute of International Affairs, 2010. ISBN 978-1-86203-243-9.

když jí definuje jako *„získávání strategicky citlivých či strategicky významných informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy“*[29].

- Kybernetický zločin (kriminalita), pro který je kyberprostor díky své relativní anonymitě a globální povaze stále ještě atraktivním prostředím, čehož můžeme být svědky takřka denně, neboť média neustále informují o internetových podvodech, sexuálních predátorech působících na síti, projevům rasismu a xenofobie, vyhrožování aj. Známý je rovněž tzv. dark web (temná síť), překryvná síť v rámci internetu, ke které lze přistupovat pouze se specifickým softwarem a kde lze nalézt stránky s ilegálním obsahem, jako je prodej drog, zbraní, falešných dokladů, kradených kreditních karet nebo přístupy k bankovním účtům. Prostředkem směny zde často bývají tzv. kryptoměny (např. známé Bitcoin, Etherum), jejichž pohyby bývají jen obtížně dohledatelné, proto není nikterak složité realizovat zde objednávku (například na tvrdé drogy) podobně, jako v běžném e-shopu.
- Kyberterorismus. Terorismus v obecné rovině představuje násilnou formu prosazování politických zájmů stoupenců určité radikální ideologie (politické, náboženské, ekologické, separatistické, aj.), kde bývají častým cílem nevinné oběti. Kyberterorismem je pak myšlena *„trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků“*[30].
- Kybernetická válka, viz podkapitola 1.3 této diplomové práce.

Na tomto místě je příhodné na okamžik opustit kyberprostor a položit otázku, nakolik by výše uvedené kategorie hrozeb byly reálné bez jeho existence. Obecná kriminalita, terorismus, špionáž i války byly člověku známy dávno před

---

[29] viz s. 58, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[30] viz s. 59, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

příchodem kyberprostoru a mohou tedy existovat i bez něj. Kyberprostor zde tedy představuje spíše nové medium, prostor, kde mohou být tyto hrozby šířeny. Některé tyto hrozby, například útok na jaderná zařízení státu (bez ohledu na to, zda by se jednalo o útok vojenský či teroristický) mají potenciál působit nesmírné škody jak na majetku, tak na životech lidí a životním prostředí. Mají potenciál působit škody všem referenčním objektům (viz dále v této práci) – mezinárodní systém, regionální systém, stát, vnitrostátní skupiny, jednotlivci – a ve všech stávajících pěti sektorech definovaných kodaňskou školou (vojenský, politický, societální, ekonomický, kulturní), a v mnoha ohledech dokonce hrozby z těchto ostatních sektorů předčít.

1.6 Kybernetický prostor

Kybernetické útoky a kybernetická válka jsou vedeny v kybernetickém prostoru, ten je Jiráskem a kol. definován jako *„digitální prostředí, umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*[31]. Obdobnou definici nabízí Ministerstvo obrany Spojených států: *„Globální prostředí sestávající ze vzájemně propojené sítě infrastruktury informačních technologií zahrnující internet, telekomunikační sítě, počítačové systémy, procesory a řídící jednotky“*[32].

V odborné literatuře i na internetu lze dohledat nespočet různých definic, ty jsou tvořeny jak akademickými pracovníky, tak i národními či nadnárodními subjekty. Většina z těchto definic ve své podstatě koresponduje se zde uvedenými. Až na některé výjimky, většina z nich (podobně jako zde prezentované pojetí Jiráska a kol., a Ottise s Lorentsem) však postrádá lidský prvek a technologickou provázanost s reálným světem. Takové vnímání může být omezující, neboť kybernetický prostor je přímo utvářen a tedy i využíván lidmi. Představené definice mohou evokovat dojem, že kyberprostor je jakýsi abstraktní, virtuální svět, nepřesahující do reálného světa. Proto je možné

[31] viz s. 59, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
[32] viz OTTIS, Rain a Peeter LORENTS. Cyberspace: Definition and Implications. *Cooperative Cyber Defence Centre of Excellence* [online]. 2012. [cit. 16.10.2022]. Dostupné z: https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf

uvažovat o rozšíření těchto přístupů o uvedený přesah. Akceptace tohoto předpokladu lépe koresponduje s vymezením kybernetického útoku dle Tallin Manual 2,0 (předpoklad schopnosti působit reálné zranění či smrt osob nebo poškození majetku), a rovněž tak s přijetím kyberprostoru coby páté dimenze pro vedení válek ze strany globálně významných aktérů, jakými jsou Spojené státy či Severoatlantická aliance (dále v této práci).

1.7 Kybernetická bezpečnost a obrana

Problematice bezpečnosti je věnován prostor v následující kapitole, nicméně obecně je možno chápat kybernetickou bezpečnost jako stav, kdy jsou v maximální možné míře eliminovány hrozby pro daný subjekt (stát) z kybernetického prostoru.[33] Jirásek a kol. definují kybernetickou bezpečnost jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“*[34]. Podrobněji se problematice věnuje ve svém příspěvku Pačka,[35] který hovoří o třech triádách tvořících koncept bezpečnosti:

a) předcházet, detekovat, reagovat - snahou subjektů zodpovědných za zajišťování kybernetické bezpečnosti je preventivní působení a předcházení kybernetickým hrozbám. Subjekt si nicméně musí být vědom rizika úspěšného útoku, proto je nezbytné věnovat pozornost také prostředkům detekce, typicky zahrnujícím hardwarové a softwarové nástroje sloužící k monitoringu aktivit na síti a v systémech. Aby byly takové snahy opodstatněné, musí být následovány reakcí (ta může mít řadu podob – například zastavení nebo odvrácení hrozby, obnova systémů).

---

[33] viz FELIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany v rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. 2017, roč. 26, č. 3. [cit. 18.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/aktualni-ukoly-kyberneticke

[34] viz s. 57, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[35] viz PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. *Bezpečnostní teorie a praxe* [online]. 2015, č. 3. [cit. 19.10.2022]. Dostupné z: https://is.muni.cz/el/fss/podzim2018/BSS469/um/Role_statu_sken.pdf

b) lidé, procesy, technologie – tato triáda demonstruje provázanost uvedených složek kybernetické bezpečnosti, neboť ty jsou mezi sebou vzájemně propojené a ani jedna nemůže fungovat nezávisle na ostatních.
c) důvěrnost, integrita a dostupnost - bývá někdy označována jako tzv. CIA triáda (Confidentiality, Integrity, Availability) a vztahuje se především k obsahu samotnému. Důvěrností je myšleno zpřístupnění obsahu pouze oprávněným uživatelům; integritou je myšlena ochrana systémů, sítí a dat před změnami neautorizovanými osobami; dostupnost pak přístupnost k tomuto obsahu a míru použitelnosti autorizovanými osobami.

Termín kybernetická obrana je blízký termínu kybernetické bezpečnosti, a v některých případech mohou být dokonce zaměňovány, nicméně mezi těmito pojmy jsou významné kvalitativní rozdíly, které tuto záměnu znemožňují. Oddělení těchto termínů je cílem následujících řádků.

Obecně lze obranu považovat za soubor defenzivních a ofenzivních aktivit a opatření na úrovni státu.[36] Pokud se týká kybernetické obrany, Jirásek a kol. ji definují jako *„obranu proti kybernetickému útoku a zmírňování jeho následků. Také rezistence subjektu na útok a schopnost se účinně bránit“*[37]. Rozšířené pojetí kybernetické obrany předkládá Pačka, který ji chápe jako *„schopnost a možnost státu působit aktivně v kyberprostoru za využití potřebných technologických a znalostních kapacit ve směru eliminace, potlačení či předcházení závažných kybernetických útoků, které mohou přicházet jak ze zahraničí, tak z vnitrostátní úrovně“*[38].

Pačkovo pojetí oproti Jiráskovi a kol. rozšiřuje kybernetickou obranu o prvek možnosti předcházení kybernetickým útokům, tzn. reagovat dříve, než dojde k samotnému útoku. V souvislosti s tím je na místě zmínit příspěvek

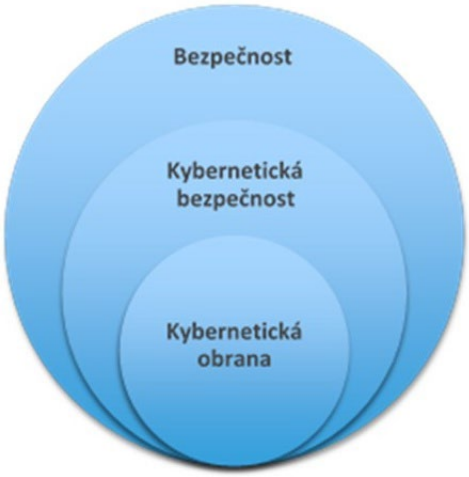
[36] viz FELIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany v rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. 2017, roč. 26, č. 3. [cit. 18.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/aktualni-ukoly-kyberneticke

[37] viz s. 58, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[38] viz PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. *Bezpečnostní teorie a praxe* [online]. 2015, č. 3. [cit. 19.10.2022]. Dostupné z: https://is.muni.cz/el/fss/podzim2018/BSS469/um/Role_statu_sken.pdf

Dawera,[39] který hovoří o aktivní a pasivní kybernetické obraně. Aktivní kybernetická obrana vyžaduje, aby měl obránce přístup k proaktivním či ofenzivním akcím vůči určité hrozbě, a rovněž tak k interakci s útočníkem, a to nejen v rámci vlastních systémů, ale také systémů útočníka. Akceptace daného rozšíření se postupem času jeví být oprávněná, o čemž koneckonců hovoří i Felix s Procházkou když konstatují, že aktivní obrana je z pohledu vojáka nedílnou součástí obrany.[40] Dalším argumentem budiž uznání kyberprostoru jakožto pátého bojiště (viz kap. 2.1), což z něj v širším pojetí dělá regulérní dimenzi nejen pro vedení válek, ale také pro realizaci preventivních obranných operací, kterým bude věnován prostor dále v této práci.

Vrátíme-li se nyní k diferencování pojmů kybernetická bezpečnost a kybernetická obrana, lze shrnout, že kybernetická obrana je součástí širší kybernetické bezpečnosti.[41] Tento vztah lze vyjádřit i graficky, jak je zobrazeno na obrázku 1.



Obrázek 1: Vztah bezpečnosti, kybernetické bezpečnosti a kybernetické obrany[42]

[39] viz DEWAR, Robert S. *Active Cyber Defense*. Zürich: Center of Security Studies [online]. 2017. [cit. 20.10.2022]. Dostupné z: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/181743/Cyber-Reports-2017-03.pdf?sequence=1&isAllowed=y

[40] viz FELIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany v rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. 2017, roč. 26, č. 3. [cit. 18.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/aktualni-ukoly-kyberneticke

[41] viz DEWAR, Robert S. *Active Cyber Defense*. Zürich: Center of Security Studies [online]. 2017. [cit. 20.10.2022]. Dostupné z: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/181743/Cyber-Reports-2017-03.pdf?sequence=1&isAllowed=y

[42] viz FELIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany v rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. 2017, roč. 26, č. 3. [cit. 18.10.2022]. ISSN 2336-

Z předchozího textu lze dovodit, že kybernetická obrana nezahrnuje ryze pasivní obranná opatření, ale pro svou efektivnost nutně vyžaduje i ofenzivní kapacity, což je fakticky v souladu s obecným pojetím obrany.

1.8 Shrnutí

Struktura podkapitol této úvodní pasáže nebyla volena náhodně. Snahou bylo postupovat od nejobecnějšího postupně až k pojmům, jakými jsou kybernetická válka, kybernetická hrozba a kybernetická obrana. Jak již bylo konstatováno, tyto pojmy mohou být zaměňovány či interpretovány nesprávně, a jelikož s nimi autor často operuje v následujícím textu, považuje jejich vymezení pro další práci za nezbytné. Stejně tak je z hlediska další práce nezbytné přenesení tradičního vojenského pojetí obrany, předpokládajícího i obranně-útočné aktivity, do prostředí kyberprostoru. Lze nicméně shrnout, že hybridní válka je rozšířeným (nikoli novým, neboť některé jeho prvky lze identifikovat již ve středověkých či starověkých konfliktech) konceptem tradiční války a jedním z jeho nástrojů je také informační válka. Informační válku je pak podle Kubeši možné chápat jako širší pojem působení na protivníka pomocí informačních technologií,[43] zatímco termíny síťová válka a kybernetická válka mohou být chápány v užším (nikoli přísně podřízeném) smyslu. Základní rozlišení mezi informační a kybernetickou válkou předkládají Arquilla a Ronfeldt,[44] dle kterých je síťová válka konfliktem na společensko-ideové úrovni, zatímco kybernetická válka na úrovni vojenské.

2995. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/aktualni-ukoly-kyberneticke

[43] viz KUBEŠA, Milan. Vojenské klamání v informačním věku. *Vojenské rozhledy* [online]. 2013, roč. 22 (54), č. 1. [cit. 17.10.2022]. ISSN 2010-3292. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/vojenske-klamani-v-informacnim-veku

[44] viz s. 27-28, ARQUILLA, John a David RONFELDT. Cyberwar is Coming! *Rand Corporation* [online]. 1993. [cit. 15.10.2022]. Dostupné z: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

2. Bezpečnostní situace 21. století

„Schopnost lidských bytostí vymýšlet nové způsoby, jak se navzájem zabíjet, se ukázala nevyčerpatelná, stejně jako naše schopnost osvobodit od milosrdenství ty, kteří vypadají jinak nebo se modlí k jinému Bohu“.

Barack Obama[45]

Od úsvitu dějin prochází lidská společnost neustálým vývojem. Významných mezníků lze identifikovat řadu, namátkou budiž jmenována například dělba práce v pracovních činnostech a počátky obchodu, rozvoj zemědělství nebo průmyslová revoluce. Počátek 21. století pak bývá často označován věkem digitálním, věkem informačních technologií nebo věkem nových médií. Termíny jsou to přinejmenším příbuzné, v mnoha ohledech zaměnitelné, a bezesporu také výstižné.

Digitální technologie vnášejí do života lidí zásadní změny. Své využití nachází takřka ve všech oblastech lidského konání, při finančních operacích, v komunikaci a dopravě, při obchodních aktivitách, ve vědě, zdravotnictví, při zábavě, ale také v průmyslu, ten vojenský nevyjímaje. Ve všech těchto aspektech přináší mnoho pozitivního, jsou hnacím motorem globální ekonomiky i výzkumu, neboť sdílení informací a myšlenek nebylo nikdy dříve tak snadné jako dnes. Počet uživatelů internetu se v roce 2022 blíží 5,5 mld. lidí, což představuje 69 % světové populace.[46]

Protože jsou tyto technologie produktem lidí – druhu, o němž hovoří úvodní citát této kapitoly převzatý z projevu bývalého amerického prezidenta Obamy u příležitosti přebírání Nobelovy ceny za mír v roce 2009 – nesou s sebou vedle těchto pozitivních (a věřme, že primárních) efektů také efekty negativní. Na straně jedné je možné hovořit o sociálních a psychických

---

[45] viz OBAMA, Barack. Remarks by the President at the Acceptance of the Nobel Peace Prize. *The White House* [online]. 2009. [cit. 13.10.2022]. Dostupné z: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize

[46] viz MINIWATTS MARKETING GROUP. World Internet Users Statistics and 2022 World Population Stats. *Internet World Stats* [online]. 2022. [cit. 16.10.2022]. Dostupné z: https://www.internetworldstats.com/stats.htm

dopadech (neboť informační technologie do značné míry ovlivňují to, jak lidé myslí a jak tráví svůj čas, vedou k omezování osobních kontaktů, apod.), a na straně druhé – a to především – mohou být využity nebo zneužity pro válečné účely či kriminální aktivity.

2.1 Kyberprostor jako specifická oblast bezpečnosti

Chceme-li uchopit problematiku využití informačních technologií pro válečné účely, je nutné úvodem stručně odbočit do oblasti mezinárodních vztahů. To je disciplína, jejíž počátky lze datovat do období po 1. sv. válce, a přestože se akademici touto problematikou zabývají již celé století, neexistuje nějaká univerzální a všezahrnující definice bezpečnosti. Rozdílnost názorů a různých pojetí bezpečnosti jsou determinovány konkrétními konceptuálními, teoretickými a časovými rámci, do nichž jsou zasazeny.[47] Z tradičního vojenskopolitického hlediska ji Baldwin jednoduše ztotožňuje s přežitím či zachováním existence, v tomto případě státu.[48] Následující stránky nicméně dokazují, že na počátku nového milénia je nutno vnímat tuto problematiku v širším kontextu.

V souvislosti s globální bezpečnostní realitou po druhé světové válce došlo k rozvoji tzv. strategických studií orientovaných na zkoumání vojenského potenciálu, poměru sil a strategických koncepcí na mezinárodní úrovni. Z důvodu jakéhosi bezpečnostního patu plynoucího z tehdejšího bipolárního uspořádání světa se do popředí zájmu teoretiků dostávají v 60. a 70. letech i otázky míru (s odhlédnutím od strategického kontextu) a minimalizace globálního střetu.[49]

Rozpad Sovětského svazu a s ním spojený konec studené války společně se zrychlujícími se globalizačními procesy podnítily koncem minulého století úvahy o novém bezpečnostním konceptu, který by reflektoval nové, příp. staronové hrozby lépe, než stávající klasické realistické přístupy. Nejvýraznějším

---

[47] viz WAISOVÁ, Šárka. Od národní bezpečnosti k mezinárodní bezpečnosti. *Global Politics: časopis pro politiku a mezinárodní vztahy* [online]. 2004, č. 3. [cit. 15.10.2022]. ISSN 1213-7685. Dostupné z: https://mv.iir.cz/article/view/124/pdf

[48] viz BALDWIN, David A. The Concept of Security. *Review of International Studies* [online]. 1997, roč. 23, č. 1. [cit. 16.10.2022]. ISSN 0260-2105. Dostupné z: https://www.cambridge.org/core/journals/review-of-international-studies/article/abs/concept-of-security/67188B6038200A97C0B0A370FDC9D6B8

[49] viz s. 22, WAISOVÁ, Šárka. *Bezpečnost – vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-21-0.

příspěvkem do diskuse o novém rámci bezpečnosti je práce Buzana a Waevra, kteří přicházejí s novým konceptem odklánějícím se od klasických státocentrických přístupů směrem k mezinárodní společnosti, jenž více vyhovuje dynamice geopolitického vývoje devadesátých let. Jde o tzv. kodaňskou školu, vymezující jak větší množství referenčních objektů, tak i větší množství hrozeb.[50]

Ve snaze o rozšíření konceptu bezpečnosti se zastánci kodaňského přístupu pohybují po dvou osách, kde na vertikální osu umisťují referenční objekty (tzn. o čí bezpečnosti je uvažováno – mezinárodní systém, regionální systém, stát, vnitrostátní skupiny, jedinci) a na horizontální zdroje hrozeb (tedy bezpečnost před čím – sektor vojenský, politický, societální, ekonomický, kulturní).[51] Bezpečnost lze pak zkoumat mezi všemi uvedenými aktéry i zdroji hrozeb.

Kodaňská konstrukce bezpečnostního konceptu je mezi odbornou veřejností poměrně široce akceptována, neboť v rámci výzkumu bezpečnosti je v 21. století nezbytné překročit tradiční vojenské pojetí bezpečnosti. Výmluvným příkladem může být tzv. ekonomická či energetická válka západního společenství s Ruskem v reakci na ruskou invazi na Ukrajině v roce 2022, kdy pomocí ekonomických a politických nástrojů (a ve své podstatě také prostřednictvím informačních technologií) znesvářené strany ohrožují bezpečnost takřka všech definovaných aktérů, tedy jak mezinárodního a regionálního systému, jednotlivých států, tak i vnitrostátních skupin či jednotlivců. Přesto Waisová[52] upozorňuje, že má i řadu kritiků, neboť vede k mnohoznačnosti a nejednoznačnosti a je nutné se ptát, kde hledat hranice bezpečnosti.

Oprávněnost diskusí o těchto hranicích podtrhují další autoři Hansen a Nissenbaum, kteří ve svém příspěvku teoretizují o kybernetické bezpečnosti jako o samostatném sektoru s konkrétními druhy hrozeb.[53] Ten ve své podstatě

---

[50] viz s. 17, BUZAN, Barry, Ole WAEVER a Jaap DE WILDE. *Bezpečnost: Nový rámec pro analýzu*. Brno: Centrum strategických studií, 2005. ISBN 80-903333-6-2.
[51] viz WAISOVÁ, Šárka. Od národní bezpečnosti k mezinárodní bezpečnosti. *Global Politics: časopis pro politiku a mezinárodní vztahy* [online]. 2004, č. 3. [cit. 15.10.2022]. ISSN 1213-7685. Dostupné z: https://mv.iir.cz/article/view/124/pdf
[52] tamtéž.
[53] viz HANSEN, Lene a Helen NISSENBAUM. Digital Disaster, Cyber Security, and the Copenhagen school. *International Studies Quartely* [online]. 2009, roč. 53, č. 4. [cit. 16.10.2022].

prostupuje ostatními pěti sektory definovanými kodaňskou školou, nicméně lze si představit řadu specifických hrozeb, které odtud mohou pramenit. Může se jednat například o vedení informační války, kyberšpionáž nebo o útok na kritickou infrastrukturu státu. Jak uvádí Pačka, *„současná infrastruktura státu je od dodávek elektřiny až po volby do parlamentu digitalizovaná a připojená k internetu. Stát, potažmo jeho vláda, jako tvůrce bezpečnostní politiky státu, se tím pádem musí obávat hrozby nejen fyzických, ale i kybernetických útoků na svou kritickou infrastrukturu“*[54]. O kybernetických hrozbách pojednává podrobněji kapitola 1.5 této práce.

„Kybernetické hrozby, které ohrožují národní a veřejnou bezpečnost a ekonomiku státu, představují jednu z nejnebezpečnějších výzev pro náš národ“[55], stojí v Národní bezpečnostní strategii Spojených států z roku 2010, která dále považuje kyberprostor za pátou doménu (vedle země, vzduchu, moře a vesmíru), kde je v případě nutnosti možné použít vojenskou sílu. Tento dokument, společně s řadou dalších, lze považovat za zřetelné vyvrcholení teoretických úvah o pojetí bezpečnosti nastíněných v předchozí podkapitole, a za jejich opodstatnění. Podobně i Severoatlantická aliance na varšavském summitu v roce 2016 uznala kybernetický prostor jako doménu, které je při obraně nutné věnovat stejnou pozornost, jako obraně ve vzduchu, na zemi i na moři.[56]

2.2 Informační revoluce

Informační revoluce odráží pokrok ve vývoji počítačů, informačních a komunikačních technologií, a souvisejících inovací v oblasti organizace a řízení. Je to fenomén, jehož počátky lze hledat přibližně v polovině 20. století a spojovat s rozvojem pokročilé elektroniky, včetně komponent počítačů,

---

ISSN 1468-2478. Dostupné z: https://is.muni.cz/el/fss/podzim2020/IREb1007/84255154/11._digital_disaster.pdf

[54] viz PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. *Bezpečnostní teorie a praxe* [online]. 2015, č. 3. [cit. 19.10.2022]. Dostupné z: https://is.muni.cz/el/fss/podzim2018/BSS469/um/Role_statu_sken.pdf

[55] viz s. 27, THE WHITE HOUSE. National Security Strategy. *The White House* [online]. 2010. [cit. 17.10.2022]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[56] viz NATO. Cyber Defence. *North Atlantic Treaty Organization* [online]. 2022. Dostupné z: https://www.nato.int/cps/en/natohq/topics_78170.htm

zobrazovacích zařízení a audiosystémů. Významným mezníkem byl rovněž vynález předchůdce dnešního internetu v roce 1969, tzv. ARPANET, kdy byly propojeny počítače na čtyřech amerických univerzitách (Stanford, Utah, Santa Barbara, Los Angeles) a došlo k přenosu textové zprávy mezi těmito počítači, či zpřístupnění internetu i komerčním subjektům počátkem 90. let minulého století.[57] V posledních letech je pak možno hovořit o rozvoji mobilních technologií nebo tzv. smart zařízení. Je tedy patrné, že se jedná o stále pokračující trend, a příklady prorůstání těchto technologií do života běžných lidí jsou patrny doslova všude kolem nás.

Pojem informační revoluce v sobě ale nezahrnuje pouze vývoj samotných technologických prostředků, ale také změn, které tyto prostředky přinášejí do naší společnosti. V důsledku enormního poklesu nákladů spojených s přenosem informací je jejich šíření mnohem jednodušší a rychlejší. Informační revoluce tak překračuje hranice států a umožňuje redistribuci moci takovým způsobem, že světová politika přestává být pod výlučnou dominancí vlád. Umožňuje zapojení jednotlivců nebo organizací, jakými jsou WikiLeaks, Anonymous, teroristické organizace, různá sociální hnutí apod.[58] Podle Arquilly a Ronfeldta[59] tak na straně jedné dochází k erozi tradičních hierarchických struktur, na kterých jsou instituce vytvořeny, na straně druhé je pak přenášen význam na všechny formy síťového uspořádání bez ohledu na to, zda se jedná o sítě sociální, komunikační či multiorganizační. Rozdíl mezi tradiční hierarchickou strukturou a multiorganizační strukturou spatřují autoři především ve způsobu jejich jednání, kdy tradiční instituce (zejména ty velké) jednají samostatně na vlastní pěst, zatímco multiorganizační sítě sestávají z často malých organizací, které se spojily za účelem společného úsilí. Informační revoluce pak podporuje růst takových sítí tím, že umožňuje různým rozptýleným aktérům koordinaci

[57] viz KLEINROCK, Leonard. An Early History of the Internet. *IEEE Communications Magazine* [online]. 2010, roč. 48, č. 8. [cit. 16.11.2022]. ISSN 1558-1896. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5534584

[58] viz NYE, Josepf S. The Information Revolution Gets Political. *Belfer Center for Science and International Affairs* [online]. 2013. [cit. 13.11.2022]. Dostupné z: https://www.belfercenter.org/publication/information-revolution-gets-political

[59] viz s. 27, ARQUILLA, John a David RONFELDT. Cyberwar is Coming! *Rand Corporation* [online]. 1993. [cit. 15.10.2022]. Dostupné z: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

a fungování na větší vzdálenosti a na základě většího množství kvalitnějších a rychlejších informací. Má tedy také transformační účinek, protože narušuje staré způsoby myšlení a fungování a poskytuje příležitost dělat věci jinak.

Jestliže byla v předešlé kapitole zmíněna kritická infrastruktura státu, je vhodné na tomto místě zmínit rovněž koncept Průmysl 4.0, jež lze velmi jednoduše popsat jako digitalizaci průmyslu. Termín, který se poprvé objevil na veletrhu v německém Hannoveru v roce 2013, vyjadřuje podle Mařík[60] transformaci výroby ze samostatných automatizovaných jednotek na plně integrovaná a průběžně optimalizovaná výrobní prostředí, kde budou hlavní roli hrát tzv. kyberneticko-fyzické systémy (Cyber Psychical Systems, CPS). Ty mají být základním prvkem inteligentních továren a mají být schopny autonomní výměny informací nebo vyvolání potřebných akcí v reakci na aktuální podmínky. Zavedení těchto principů by podle Mařík mělo pomoci předvídat případné chyby či poruchy nebo se rychleji adaptovat v nastalých podmínkách, v důsledku čehož má být dosaženo vyšší flexibility a efektivity výroby. Tento koncept je zde zmíněn ze dvou důvodů. Krom toho, že je příkladnou ukázkou praktického prorůstání digitálních technologií do všech oblastí lidského konání, vyvolává také otázku, nakolik by zneužití či napadení takového systému mohlo být nebezpečné, zejména týká-li se oblastí souvisejících s kritickou infrastrukturou státu (například energetika).

Všechny tyto skutečnosti se přímo dotýkají také organizace armády, či v širším pojetí vedení konfliktů a válek. Způsob vedení boje již není založen pouze na tom, která ze stran disponuje nejpočetnější armádou či nejmodernějšími technologiemi, ale také na tom, která strana má nejlepší informace o bojišti, a jak je dovede využít.[61]

2.3 Revoluce ve vojenských záležitostech

Podobně, jako tomu bylo v případě předešlých dvou kapitol, jeví se z hlediska zkoumané problematiky jako přínosné přiblížit rovněž vývoj přístupu

---

[60] viz s. 27, MAŘÍK, Vladimír. *Průmysl 4.0: Výzva pro Českou republiku*. Praha: Management Press, 2016. ISBN 978-80-7261-440-0.
[61] viz s. 23, ARQUILLA, John a David RONFELDT. Cyberwar is Coming! *Rand Corporation* [online].1993. [cit. 15.10.2022]. Dostupné z: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

k vojenským záležitostem. Není to jen společnost sama o sobě, její geopolitická a bezpečnostní situace, vzájemné vztahy mezi národy či technologické prostředky, které se vyvíjejí. Na všechny tyto dynamicky se vyvíjející výzvy musí reagovat také vojenský sektor a uzpůsobovat jim své strategie a doktríny. Z historických příkladů je možno jmenovat využití jízdních jednotek ve starověkých válkách, vynález střelného prachu a palných zbraní, bojových letadel nebo jaderných zbraní.

Vrátíme-li se do období studené války, problematikou revoluce ve vojenských záležitostech se poprvé zabývali sovětští stratégové od 70. let minulého století v návaznosti na postupné zavádění nových zbraňových a informačních technologií (jaderné zbraně, přesně naváděná munice, prostředky dálkového průzkumu aj.) především ze strany Spojených států coby jejich významného rivala. Ti došli k poznání, že v důsledku uvedených změn dojde k proměně tradičního způsobu vedení boje, a rozpracovali koncept tzv. vojensko-technické revoluce (Military-Technical Revolution, MTR). Na tyto úvahy postupně navázali američtí analytici a rozšířili ryze technologické pojetí o další faktory, především o organizační změny, čímž de facto redefinovali vojensko-technologickou revoluci na tzv. revoluci ve vojenských záležitostech (Revolutions in Military Affairs, RMA). Teoretikové došli k závěru, že RMA významným způsobem ovlivňuje efektivitu boje, především díky technologické změně, operačním a organizačním inovacím.[62] Gray[63] identifikuje pět fází vývoje RMA:

1. počáteční fáze identifikace sovětskými stratégy, popsané v předešlém odstavci;
2. modifikace amerických teoretiků;
3. vyvrcholení zkoumání RMA ve smyslu obdivu k pokročilým technologiím;
4. zavedení myšlenek RMA do praxe, jehož počátky lze datovat do období působnosti bývalého amerického prezidenta G. W. Bushe;
5. pochyby o přílišném soustředění a spoléhání se na technologická řešení strategických výzev, jednak z důvodu přílišných nákladů, a dále sílící po

[62] viz s. 24, FUČÍK, Jakub. *Vývoj konceptu současné revoluce ve vojenských záležitostech*. Brno, 2017. Disertační práce. Masarykova Univerzita, Fakulta sociálních studií, Katedra mezinárodních vztahů a evropských studií. Vedoucí práce doc. PhDr. Zdeněk Kříž, Ph.D.
[63] viz s. 114-119, GRAY, Colin S. *Strategy and History: Essays on Theory and Practice*. London: Routledge, 2006. ISBN 978-0-415-38635-7.

konfliktech v Iráku a Afganistánu, kde navzdory naprosté technologické dominanci Spojených států bylo problematické čelit houževnatému partyzánskému odporu využívajícího výhod terénu.

Fučík dále hovoří o aktuálně probíhající šesté fázi, charakteristické zpomalováním výše uvedených trendů.[64] Nutno ovšem zdůraznit, že zpomalování trendu automaticky neimplikuje komplexní odklon od tohoto trendu. To je patrné mimo jiné i z výstavy, která pod názvem AUSA 2022 proběhla v říjnu roku 2022 ve Washingtonu, demonstrující, jak si Amerika představuje válku budoucnosti – mikrovlnné systémy protivzdušné obrany, autonomní pozemní i vzdušní bezpilotní roboti aj.

2.4 Shrnutí

Je-li řeč o válce, lidé mají většinou tendenci uvažovat o pojmech, které jsou základem klasické války, potažmo vyhrožování touto klasickou válkou – početnost armády, množství techniky, apod. Tuto skutečnost lze opět ilustrovat na příkladu právě probíhající války na Ukrajině. V jejích počátcích světová média (a jimi oslovení analytici) předkládala srovnání počtu vojenské techniky a živé síly na obou stranách konfliktu a spekulovala o „pádu Kyjeva během několika dnů“ či „hladkém vítězství Ruska“. Jakoby přitom zapomínala na další aspekty boje, jakými je odhodlání a vlastenecké cítění úzce spojené s pojmem informační války nebo sílu politických a ekonomických prostředků nátlaku.

Jak ale dokládá předešlý text, v 21. století představují vojenské zdroje o mnoho více. Snahou autora bylo v rámci předešlých třech podkapitol nahlédnout vývoj posledního půlstoletí z několika perspektiv – pohledem obecného technologického pokroku, reakce teorie mezinárodních vztahů na tento pokrok, a rovněž tak perspektivou vojenskou. Všechny tyto pasáže pak dokládají, že v 21. století musí být toto tradiční chápání rozšířeno. Aneb, jak uvádí Nye, *„z 226 významných ozbrojených konfliktů mezi léty 1945 a 2002 byla necelá polovina z nich vedena mezi státy a ozbrojenými skupinami. Občanská válka a neregulérní bojovníci samozřejmě nejsou novinkou, jak uznává i tradiční*

[64] viz s. 49, FUČÍK, Jakub. *Vývoj konceptu současné revoluce ve vojenských záležitostech*. Brno, 2017. Disertační práce. Masarykova Univerzita, Fakulta sociálních studií, Katedra mezinárodních vztahů a evropských studií. Vedoucí práce doc. PhDr. Zdeněk Kříž, Ph.D.

válečné právo. Co je nové, je nárůst nepravidelných armád a technologické změny, které dávají stále větší destruktivní sílu do rukou malých skupin. A nyní technologie přinesla do válčení nový rozměr: vyhlídky na kybernetické útoky, pomocí kterých může nepřítel, státní i nestátní, způsobit obrovskou fyzickou likvidaci, aniž by armáda fyzicky překročila hranici jiného státu"[65]*.* Nye těmito slovy komentuje nasazení jedné z nejznámějších kybernetických zbraní – Stuxnet. Viru, který dokázal napadnout závod izolovaný uprostřed pouště a odpojený od internetu s cílem nepozorovaně působit obrovské škody z kybernetického prostoru ve světě reálném. A zřejmě přitom také platí, že jeho nasazení bylo humánnější alternativou ozbrojeného útoku, který by byl bezesporu zaplacen lidskými životy, v horším případě pak rozbuškou pro větší regionální konflikt. Podrobnostmi tohoto případu se zabývá následující část práce.

[65] viz NYE, Joseph S. Is Military Power Becoming Obsolete? *Project Syndicate* [online]. 2010. [cit. 13.11.2022]. Dostupné z: https://www.project-syndicate.org/commentary/is-military-power-becoming-obsolete-2010-01?barrier=accesspaylog

II. ANALYTICKÁ ČÁST

3. Konflikt Spojené státy-Írán

Praktická část práce se zabývá případovou studií sporu mezi Spojenými státy a Islámskou republikou Írán ohledně utajovaného íránského jaderného programu, který přerostl v konflikt vedený v kybernetickém prostoru a demonstrující schopnosti moderních kybernetických zbraní. Cílem práce je ověření hypotézy, že mezi Spojenými státy a Íránem probíhá plnohodnotná kybernetická válka.

Ve snaze o co možná nejpřesnější obraz konfliktu autor nejprve popisuje vývoj situace v Íránu přibližně od poloviny minulého století formující současné protizápadní postoje režimu a okolnosti vedoucí k obavám, že Teherán usiluje o získání jaderné zbraně, stejně jako místy až absurdní snahy tento vývoj ututlat před mezinárodním dohledem. To představuje kontext celého incidentu. Významná část práce je dále věnována popisu malwaru Stuxnet, jeho vývoji, způsobu nasazení a škodám, jaké dovedl cílovému subjektu napáchat. Následně se autor zabývá reakcí Íránu na tento útok, a to jak na poli budování vlastních kybernetických sil íránského režimu, tak i z hlediska jejich reálných schopností. Zvláštní důraz je přitom vždy věnován motivaci útočníků a důkazům či výpovědím zainteresovaných jedinců hovořících o vazbách útočníků na íránskou vládu. Na základě těchto skutečností je v závěrečné části testována výše prezentovaná hypotéza.

Případová studie se opírá především o informace z odborné, převážně cizojazyčné literatury, webových stránek zainteresovaných institucí, zpráv publikovaných organizacemi zabývajícími se kybernetickou či mezinárodní bezpečností, a dále pak čerpá z článků zahraničních zpravodajských serverů dokumentujících jednotlivé kybernetické útoky.

Překážkou při zpracování případové studie byla poměrně značná absence oficiálních íránských stanovisek nebo důležitých dat. Příčinou může být jednak

samotná jazyková bariéra, jednak značná disproporce v objemu amerických (či šířeji západních) a íránských materiálů.

3.1 Počátek konfliktu

Aby bylo možné hodnotit vztah obou zkoumaných aktérů, příp. míru závažnosti konfliktu mezi nimi, je nutné nejprve udělat krátký exkurz do historie Blízkého východu. Předmětem zájmu následujících stránek je zejména Islámská republika Írán, její jaderný program a s ním související změna politické orientace země, vyvolaná tzv. islámskou revolucí. Právě zde lze totiž spatřovat počátky americko-íránského konfliktu.

Oblast Blízkého východu je sama o sobě velmi nestabilním regionem s řadou třaskavých míst a specifických regionálních problémů. Významným aktérem této oblasti je právě Írán, který bývá v odborné literatuře, na politických fórech, i v oficiálních zprávách ministerstev či zpravodajských služeb označován za největšího státního podporovatele terorismu na světě s vlastním jaderným programem.[66] Dle zprávy z roku 2020 země vynakládá okolo 1 mld. USD na podporu teroristických činů každý rok.[67] Abychom tuto skutečnost uvedli do kontextu, celkové armádní výdaje České republiky dosahují zhruba čtyřnásobné výše, přičemž HDP na obyvatele generuje Česká republika ve srovnání s Íránem přibližně trojnásobný.[68]

Je poněkud paradoxní, že na počátku íránského jaderného programu stály Spojené státy, které jsou v současnosti jeho největším odpůrcem. Ačkoli Írán zahájil svůj jaderný program v polovině 50. let minulého století (roku 1957 podepsaly Spojené státy s Íránem dohodu o civilní jaderné spolupráci v rámci amerického programu Atmos for Peace[69]), rozvíjel se velmi pozvolna až do konce 60. let, kdy Írán od Spojených států získal experimentální reaktor o výkonu 5 MW pro své výzkumné a výukové centrum na Teheránské univerzitě.

---

[66] viz s. 34, KRAUS, Josef. *Íránský státní terorismus: Od Chomejního po Ahmadínežáda*. Brno: Centrum pro studium demokracie a kultury, 2014. ISBN 978-80-7325-342-4.
[67] viz s. 9, KING FAISAL CENTER FOR RESEARCH AND ISLAMIC STUDIES. *Iran's Cyberattacks Capabilities.* Riyadh: KFCRIS, 2020.
[68] viz BUSINESSINFO.CZ. *Írán*. [online]. 2022. [cit. 5.2.2023]. Dostupné z: https://www.businessinfo.cz/navody/iran-souhrnna-teritorialni-informace/2/
[69] viz JAHANPOUR, Farhang. Chronology of Iran's Nuclear Programme, 1957-2007. [online]. 2007. [cit. 29.12.2022]. Dostupné z: https://www.oxfordresearchgroup.org.uk/work/middle_east/iranchronology.php

Dohoda obsahovala technickou pomoc ze strany USA, dodávky obohaceného uranu pro mírové účely, a rovněž tak předpokládala budoucí spolupráci na poli mírového využití jaderné energie. V roce 1968 společně s dalšími zeměmi podepsal Írán Smlouvu o nešíření jaderných zbraní (Nuclear Non-Proliferation Treaty – NPT), která byla ratifikována vládou v roce 1970. Obohacování uranu bylo podle smlouvy povoleno.[70] V následujících letech bylo uzavřeno několik větších kontraktů na výstavbu jaderných závodů a dodávky jaderného paliva, zejména se Spojenými státy, Francií a Německem. Nutno zdůraznit, že veškeré tyto aktivity směřovaly k mírovému využití jádra. V roce 1974 podepsal Írán dohodu s IAEA, která obsahovala záruky umožňující inspekce za účelem ověření, že jaderné obohacování pro mírové účely není nikterak zneužíváno pro vývoj jaderné zbraně.[71]

Zlom nastal až v roce 1979, kdy islámská revoluce v Íránu ukončuje jeho jaderný program. Společně s tím byla ukončena spolupráce se Spojenými státy, v důsledku čehož přestaly Spojené státy dodávat obohacený uran pro teheránský reaktor.[72] Samotná íránská islámská revoluce je považována za jednu z nejvýznamnějších vnitropolitických událostí novodobých íránských dějin. Při střetech mezi příznivci dosavadního vládce šáha Muhammada Rezy Pahlavího a exilového opozičního vůdce Ajatolláha Chomejního bylo zabito či umučeno několik tisíc lidí. Ve velkém byly také podnikány útoky na místa a symboly, které mají spojitost se západní kulturou.[73] Revoluce byla zřetelným příkladem toho, že íránská společnost neměla zájem o americkou kulturu a hodnoty ani o prozápadně orientovaného šáha. Chomejní zastával vůči jaderné energii zdrženlivý postoj, ze země odešla řada jaderných expertů, a kvůli nedostatečné infrastruktuře, protizápadním náladám a poklesu zisků z ropy odešli také významní zahraniční partneři.

---

[70] viz s. 298, CIRINCIONE, Josepf. *Repairing the Regime: Preventing the Spread of Weapons of Mass Destruction*. New York, London: Routledge, 2000. ISBN 0-415-92595-9.
[71] viz JAHANPOUR, Farhang. Chronology of Iran's Nuclear Programme, 1957-2007. [online]. 2007. [cit. 29.12.2022]. Dostupné z: https://www.oxfordresearchgroup.org.uk/work/middle_east/iranchronology.php
[72] viz JAHANPOUR, Farhang. Chronology of Iran's Nuclear Programme, 1957-2007. [online]. 2007. [cit. 29.12.2022]. Dostupné z: https://www.oxfordresearchgroup.org.uk/work/middle_east/iranchronology.php
[73] viz s. 90 – 92, CVRKAL, Zdeněk. *Írán – stručná historie státu*. Praha: Libri, 2007. ISBN 978-80-7277-337-4.

Od počátku svého působení byla íránská revoluční vláda nucena čelit vedle vnitřní nestability také problémům vnějším. Invaze Iráku a ztráta nejmocnějšího spojence (Spojených států) významně přispěly k pocitu politické a vojenské zranitelnosti Íránu. Válka s Irákem (či spíše náhlý útok Iráku) trvající od roku 1980 do roku 1988, mnohočetné bombardování jaderné elektrárny v Búšehru, chemické útoky proti tisícovkám íránských vojáků, raketové útoky na íránská města a celkové vyčerpání zdrojů mělo na Írán devastující dopad.[74] Odhaduje se, že během konfliktu přišlo o život asi 1,5 mil. lidí.[75] Navíc se Írán cítil být ohrožen rostoucími jadernými kapacitami sousedního Iráku. Saddám Husajn se koneckonců nikterak netajil zájmem nahradit Írán v pozici regionální mocnosti.[76] Tyto skutečnosti poskytují vysvětlení, proč vláda Ajatolláha Chomejního nakonec v roce 1984 učinila rozhodnutí vrátit se k pokračování v jaderném programu, a ještě dále posílila jaderný výzkum. Jestliže předrevoluční jaderný program v Íránu těžil ze spolupráce se západními partnery (především zmiňované Spojené státy, Německo, Francie), po revoluci se íránští představitelé orientovali na východ. V roce 1989 byl podepsán desetibodový pakt o spolupráci mezi Íránem a Ruskem o mírovém využití jaderného materiálu a souvisejícího vybavení, v následujících letech pak byl domluven odkup několika reaktorů od Číny. Roku 1993 Německo odmítlo dokončit výstavbu rozestavěné jaderné elektrárny v Búšehru. Důvodem bylo sílící podezření, že Írán usiluje o získání jaderné zbraně.[77] V lednu roku 1995 nicméně Rusko oznámilo, že dokončí výstavbu nedokončeného závodu v Búšehru, a souhlasilo s výstavbou tří dalších reaktorů. Americké zpravodajské služby dlouho podezíraly Írán, že využívá svůj civilní jaderný program jako zástěrku pro vývoj tajných zbraní, a americká vláda aktivně tlačila na potenciální dodavatele, aby omezili jadernou spolupráci s Íránem. V důsledku těchto snah Čína nakonec Íránu nedodala dříve domluvené komponenty a alespoň částečně ustoupilo také Rusko. Navzdory tomuto zákazu jaderné spolupráce s Íránem na nejvyšší úrovni

[74] tamtéž.
[75] viz s. 331, BROŽ, Ivan. *Husajn kontra Chomejní: irácko-íránská válka 1980-1988*. Praha: Epocha, 2007. ISBN 978-80-87027-12-7.
[76] tamtéž.
[77] viz JAHANPOUR, Farhang. Chronology of Iran's Nuclear Programme, 1957-2007. [online]. 2007. [cit. 29.12.2022]. Dostupné z: https://www.oxfordresearchgroup.org.uk/work/middle_east/iranchronology.php

se američtí představitelé domnívají, že jednotliví ruští vědci a instituce pomáhali íránským inženýrům v citlivých oblastech jaderné energetiky.[78]

Organizace Národní rada odporu Íránu (National Council of Resistance – NCRI) v roce 2002 odhalila existenci nedeklarovaných jaderných zařízení v Íránu (Natanz, Arak) společně se jmény osob a institucí zapojených do utajovaného jaderného programu.[79] V reakci na tato zjištění realizovala Mezinárodní agentura pro atomovou energii (International Atomic Energy Agency – IAEA) sérii jednání s Íránem ohledně jeho jaderného programu pro vojenské účely a provedla v souvislosti s tím řadu inspekcí.[80] Tyto opakované mise IAEA potvrdily snahu Íránu o utajování důležitých skutečností vztahujících se k jeho jadernému programu, nicméně íránští představitelé se podepsáním dodatkového protokolu zavázali ukončit aktivity odporující NPT a na chvíli se tak zdálo, že jednání směřují správným směrem.

Jak ale uvádí NTI[81], americké zpravodajské služby v roce 2004 obdržely informace, dle kterých Írán zaměřil svou pozornost na úpravu nosných raket Shahab-3, aby byly schopny nést jaderné hlavice. Téhož roku IAEA rovněž zjistila, že při předešlých inspekcích byly utajeny další informace, což bylo íránskými představiteli odmítnuto jako podvrh.

Diplomatický pokrok vzal za své v srpnu 2005, kdy IAEA zjistila, že Írán porušil její pečetě na zařízení pro konverzi uranu.[82] Írán zároveň oznámil, že obnoví aktivity související s obohacováním uranu v Esfahánu, a odmítl dohodu s trojicí evropských států (Francie, Německo, Velká Británie) zvanou EU-3 s odůvodněním, že tato dohoda klade na režim vysoké požadavky, je slabá na pobídky a nerespektuje íránská stanoviska ani Pařížskou dohodu. Dne 28. června 2005 podepsal prezident George W. Bush výkonný příkaz, který blokuje

---

[78] viz NTI. Iran Nuclear Overview. *NTI* [online]. 2020. [cit. 1.1.2023]. Dostupné z: https://www.nti.org/analysis/articles/iran-nuclear/
[79] tamtéž
[80] viz ŠEVEČEK, Martin. Íránský jaderný program – vznik sankcí, současnost a budoucnost. *OENERGETICE.CZ* [online]. 2016. [cit. 1.1.2023]. Dostupné z: https://oenergetice.cz/ropa/iransky-jaderny-program-je-pod-kontrolou-co-nas-ceka-dal
[81] viz NTI. Iran Nuclear Overview. *NTI* [online]. 2020. [cit. 1.1.2023]. Dostupné z: https://www.nti.org/analysis/articles/iran-nuclear/
[82] viz ŠEVEČEK, Martin. Íránský jaderný program – vznik sankcí, současnost a budoucnost. *OENERGETICE.CZ* [online]. 2016. [cit. 1.1.2023]. Dostupné z: https://oenergetice.cz/ropa/iransky-jaderny-program-je-pod-kontrolou-co-nas-ceka-dal

finanční aktiva subjektů podporujících výrobu zbraní hromadného ničení.[83] V únoru 2006 sdělují představitelé Íránu IAEA, že země přestane dobrovolně implementovat dodatkový protokol a další nezávazné inspekční postupy, o dva měsíce později pak informují, že země poprvé obohatila uran v zařízení v Natanzu.[84]

V prosinci roku 2006 rozhodla Rada bezpečnosti OSN o zákazu importu a exportu materiálů a zařízení souvisejících s jaderným programem a o zmrazení účtů organizací a osob spojených s tímto programem. I přes snahy IAEA o pozastavení íránských aktivit nedošlo ke splnění stanovených podmínek, a tak přišlo v březnu 2007 druhé, tvrdší kolo sankcí. V létě 2007 vypracovala IAEA plán, jak situaci řešit. Íránská strana začala více spolupracovat a inspektoři IAEA provedli několik misí včetně kontroly těžkovodního reaktoru v Araku, kde mělo probíhat tzv. množení štěpného materiálu s cílem tvorby plutonia. Vyjednávání o ukončení íránských aktivit bylo neúspěšné, a tak v březnu 2008 začalo třetí kolo sankcí. Írán navíc začal stavbu nových obohacovacích závodů v roce 2009. Oficiálním cílem bylo získání obohaceného uranu pro jejich výzkumné reaktory. V reakci na to USA, Rusko a Francie nabídli, že jaderné palivo Íránu dodají sami. Další přitvrzení sankcí přišlo v červnu 2010, kdy došlo ze strany Íránu také k napadení schopností inspektorů IAEA a jejich vyhoštění.[85]

Přestože výše uvedené skutečnosti jsou jen výtahem těch událostí, které se z pohledu autora práce jeví jako nejzásadnější, zřetelně vykreslují Írán jako kontroverzního a nepříliš solventního partnera pro jakékoli jednání či spolupráci. Bez ohledu na to, zda je řeč o podpoře terorismu ze strany íránských představitelů (zejména v době, kdy západní společenství vyhlásilo válku terorismu po útocích z 11. září 2001), utajovaném íránském jaderném programu (či kombinaci těchto faktorů, neboť mnohé zločinecké skupiny nepochybně usilovaly o získání tzv. špinavé bomby) nebo silných protizápadních postojích

---

[83] viz NTI. Iran Nuclear Overview. *NTI* [online]. 2020. [cit. 1.1.2023]. Dostupné z: https://www.nti.org/analysis/articles/iran-nuclear/

[84] DAVENPORT, Kelsey. Timeline of Nuclear Diplomacy with Iran. *Arms Control Association* [online]. 2022. [cit. 3.1.2023]. Dostupné z: https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran

[85] viz ŠEVEČEK, Martin. Íránský jaderný program – vznik sankcí, současnost a budoucnost. *OENERGETICE.CZ* [online]. 2016. [cit. 1.1.2023]. Dostupné z: https://oenergetice.cz/ropa/iransky-jaderny-program-je-pod-kontrolou-co-nas-ceka-dal

a výrocích hraničících s vyhrožováním (jimiž proslul zejména Mahmud Ahmadínežád, který byl inaugurován šestým prezidentem Íránu v roce 2005), zpochybňování geopolitického rozložení moci či legitimity OSN, agresivní rétoriku vůči sousedními Izraeli spojenou s popíráním holocaustu. Nelze se proto divit, že mnozí autoři hovoří o úvahách předních světových vůdců (zejména představitelů Spojených států či Izraele) o přímé vojenské intervenci. Uvažováno mělo být o leteckém úderu, který by z hlediska mezinárodního společenství mohl být problematický.[86]

3.2 Stuxnet

„17. června 2010 si zaměstnanci běloruské společnosti VirusBlokAda všimli, že počítač jejich íránského zákazníka se chová divně a neustále se restartuje. Po chvíli se jim podařilo izolovat nákazu a užasli. Nejen, že se jednalo o zcela nový typ malware, ale červ navíc používal k infekci počítačů velmi netradiční metodu – USB disk v kombinaci s do té doby s neznámou bezpečnostní dírou (tzv. 0-day útok) Windows Exploreru, díky níž bylo možné počítač nenápadně infikovat při prohlížení obsahu nově připojeného disku. Malware používající doposud neznámou bezpečnostní slabinu je poměrně vzácný – typicky se objevuje jen asi v jednom z milionu případů nově objevených hrozeb. Časem se mělo ukázat, že červ, který napadl počítače v Íránu, je ještě o několik řádů vzácnější – využíval totiž pro své šíření čtyři různé 0-day slabiny a dva ukradené bezpečnostní certifikáty pro instalaci současně. Byl tak vlastně sofistikovanější, než miliony každoročně se objevujících nákaz dohromady“, přibližuje ve svém příspěvku Erben okolnosti objevení a sofistikovanost červa Stuxnet.[87] Autor dále uvádí, že poté, co byla ve spolupráci s Microsoftem připravena záplata, byly informace o objevení zveřejněny. Pojmenování Stuxnet bylo odvozeno z názvů souborů obsažených v jeho kódu.

---

[86] viz s. 708, SOLIS, Gary D.*The Law of Armed Conflict: International Humanitarian Law in War*. 2nd ed. Cambridge: Cambridge University Press, 2016. ISBN 978-1-107-13560-4.
[87] viz ERBEN, Lukáš. Příchod hackerů: příběh Stuxnet. *Root.cz* [online]. 2014. [cit. 3.1. 2023]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

Sanger[88] (ale i další autoři, například výše citovaný Erben) chápe Stuxnet jako součást rozsáhlejší operace pod názvem „Olympijské hry“, kterou spustila administrativa bývalého amerického prezidenta George W. Bushe v roce 2006. Stěžejním cílem této operace bylo prostřednictvím sabotáží a kybernetických útoků oslabit, zpomalit nebo zcela zastavit íránský jaderný program. Patrně se také jednalo o způsob, jak přesvědčit Izrael, aby opustil své plány na konvenční útok proti íránským jaderným zařízením.[89] Na této operaci se podílely agentury Spojených států Národní bezpečnostní agentura (The National Security Agency – NSA), jejíž hackeři ze skupiny Tailored Access Operation (TAO) měli naprogramovat značnou část kódu Stuxnetu, a Ústřední zpravodajská služba (Central Intelligence Agency - CIA) spolu s Izraelskou kybernetickou kanceláří Unit 8200.[90] Operace spočívala v provedení kybernetického útoku na cíl, který je přísně střežen a navíc odříznut od internetu. Skupina hackerů TAO byla i přesto schopna si s tímto poradit a dokázala nalézt síťový vstup do dané oblasti, který bezpečnostní programátoři opomenuli.

První fází byl vývoj počítačového kódu, který bude možné vložit do počítačů vyrobených německou společností Siemens a zmapovat jejich provoz, vytvořit jakýsi ekvivalent elektronického plánu závodu v Natanzu, aby útočníci získali informace o způsobu řízení zdejších odstředivek. Následně musel být program schopen poslat získané informace do ústředí NSA. Teprve poté bylo možné zahájit vývoj nesmírně složitého počítačového červa, který by se stal útočníkem zevnitř. Druhou fází operace bylo vytvoření samotného červa a jeho následné testování. Spojené státy za tímto účelem vybudovaly za nejpřísnějšího utajení jakousi virtuální repliku závodu v Natanzu s využitím odstředivek pocházejících z programu libyjského diktátora Muammara Kaddáfího. Sanger popisuje, že ke konci funkčního období prezidenta Bushe byly na konferenčním stole v situační místnosti rozloženy trosky centrifugy jakožto důkaz potenciální

---

[88] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[89] viz ERBEN, Lukáš. Příchod hackerů: operace Olympijské hry. *Root.cz* [online]. 2014. [cit. 3.1. 2023]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-operace-olympijske-hry/

[90] viz s. 708, SOLIS, Gary D.*The Law of Armed Conflict: International Humanitarian Law in War*. 2nd ed. Cambridge: Cambridge University Press, 2016. ISBN 978-1-107-13560-4.

síly nové kybernetické zbraně. Stuxnet byl připraven k nasazení proti skutečnému cíli - íránskému podzemnímu obohacovacímu závodu.[91] Michael V. Hayden, bývalý šéf CIA, prohlásil: *„Předchozí kybernetické útoky měly účinky omezené na jiné počítače. … Jedná se o první útok velkého rozsahu, ve kterém byl kybernetický útok použit k fyzickému ničení“*[92].

Způsob, jakým byl pečlivě připravený červ dopraven do Natanzu, popisuje ve svém díle Kaplan.[93] Využito zde bylo vazeb s izraelskou tajnou službou Mossad, kdy byl prostřednictvím špionů USB disk dopraven přímo do areálu jaderného zařízení.

Po zahájení upravili útočníci činnost Stuxnetu tak, aby snížili podezření ze strany íránských vědců. Pokud by zanechali program v původním nastavení, docházelo by k vysokému nárůstu explozí centrifug, což by zřejmě vyvolalo podezření. Proto upravili svůj plán a rozdělili ho na dvě fáze. V první fázi se dostali do řídícího centra ventilů centrifug, které určovaly množství uranového plynu vstupujícího do centrifug.[94] Jak doplňuje Sanger, *„první útoky byly malé, a když se centrifugy v roce 2008 začaly vymykat kontrole, byli Íránci podle odposlechů, které později zachytily Spojené státy, o příčině zmateni. … Íránci byly zmateni částečně proto, že žádné dva útoky nebyly úplně stejné. … Když červ zaútočil, vyslal signály do řídící místnosti Natanzu, které naznačovaly, že vše funguje normálně“*[95]. V druhé fázi pak přešli k řízení samotné rotace centrifug, kterou postupně navyšovali, případně snižovali, aby nedošlo k podezření.

---

[91] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[92] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[93] viz s. 96-98, KAPLAN, Fred M. *Dark Territory: The Secret History of Cyber War.* New York: Simon, 2017. ISBN 978-1-4767-6326-2.

[94] tamtéž

[95] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Do roku 2010 tento malware skrytě fungoval uvnitř elektrárny Natanz a podařilo se mu odstavit zhruba 2 000 centrifug z 8 700. V létě 2010 se Stuxnetu podařilo dostat ven do volného kyberprostoru pomocí programovací chyby.[96] Chyba v kódu způsobila, že se červ dostal do počítače jaderného inženýra, který byl v Natanzu připojen k odstředivkám. Když se tento expert připojil k internetu mimo areál závodu, červ nebyl schopen rozeznat změnu prostředí a začal se šířit i na počítače, které neměly být jeho cílem.[97] Tehdy začal být sledován některými softwarovými bezpečnostními společnostmi, Symantec v USA, VirusBlokAda v Bělorusku, Kaspersky Labs v Rusku aj. Jeho účel se podařilo odhalit až po hlubší analýze kódu. Společnosti odhalily jeho komplexnost a uvědomily si, že se jim do rukou dostal ten nejsofistikovanější počítačový červ, s jakým se doposud setkaly. Symantec během následujících tří měsíců odhalil, že účelem nebyla pouze špionáž, ale spíše samotná sabotáž.[98]

Spojené státy po odhalení fungování Stuxnetu nestáhly tento malware z íránského reaktoru, ale naopak zintenzivnily jeho průběh a zvýšily otáčky centrifug. V následujících týdnech po objevení Stuxnetu, byla elektrárna Natanz zasažena novější verzí Stuxnetu a poté ještě jednou. Za toto krátké období se podařilo odstavit až 1 000 centrifug z 5 000, které v té době nadále fungovaly.[99]

Pro úplnost je třeba dodat, že Stuxnet nebyl jediným virem, který cílil na íránská jaderná zařízení. Nedlouho po jeho objevení byly odhaleny také viry Duqu a Flame, které byly spíše průzkumnými nástroji, na rozdíl od sabotážního Stuxnetu. Přinejmenším v případě prvně jmenovaného, Duqu, existují silné indicie naznačující, že byl napsán stejnými programátory, neboť tyto viry ve svém zdrojovém kódu obsahují stejné „otisky prstů“.[100] Pokud jde o Flame, zde

---

[96] viz ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, Crown, 2014. ISBN 978-0-7704-3618-6.
[97] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[98] viz ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, Crown, 2014. ISBN 978-0-7704-3618-6.
[99] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[100] viz PERLROTH, Nicole. Researchers Link Flame Virus to Stuxnet and Duqu. *The New York Times* [online]. 2012. [cit. 16.2.2023]. Dostupné z:

výzkumníci z Kaspersky Labs vyslovili názor, že v tomto případě se jedná o program vytvořený jiným týmem programátorů, který byl ale pověřen stejným subjektem, přičemž digitální důkazy poukazují, podobně jako v případě Stuxnetu a Duqu, na společné americko-izraelské úsilí podkopat íránské snahy o výrobu jaderné zbraně.[101]

3.3 Reakce Íránu na nasazení Stuxnetu

Již v předešlé podkapitole bylo naznačeno, že ačkoli žádná země oficiálně nepřiznala svůj podíl na útoku Stuxnetu, všeobecně se má za to, že malware byl vyvinut Spojenými státy ve spolupráci s Izraelem. Velmi podrobně se operaci věnují například Solis[102] hovořící o zdrojích poskytujících potvrzující podrobnosti o zapojení programátorů z TAO, či Sanger[103] citující ve svém příspěvku i některé vysoce postavené představitele tajných služeb podílející se na útoku. Lze shrnout, že mezi odbornou veřejností není o autorství Spojených států pochyb. Obdobné závěry zřejmě vyvodili také íránští představitelé, kteří v reakci na působení Stuxnetu zahájily významné rozšiřování kybernetických kapacit země s cílem odradit potenciální útočníky od dalších obdobných útoků, těmto útokům se umět bránit a rovněž na ně adekvátně reagovat. O tom svědčí mimo jiné i výrazné navýšení kybernetických útoků z íránského území proti cílům ve Spojených státech nebo jejich blízkým spojencům bezprostředně po odhalení Stuxnetu. Přiblížení některých vybraných útoků je obsahem této kapitoly.

3.3.1 Operace Newcaster

Americká společnost iSight Partners, zabývající se kybernetickou bezpečností, zveřejnila v roce 2014 zprávu týkající se odhalení minimálně tři roky trvající kybernetické špionážní kampaně, která byla nazvána operace Newcaster. Cílila na americké vojenské dodavatele, členy Kongresu, diplomaty

---

https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html

[101] tamtéž.

[102] viz s. 708-709, SOLIS, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*. 2nd ed. Cambridge: Cambridge University Press, 2016. ISBN 978-1-107-13560-4.

[103] viz SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

a novináře.[104] Operace měla trvat minimálně tři roky a dle expertů z iSight Partners se mělo jednat o nejpropracovanější kybernetickou špionážní kampaň využívající sociální inženýrství, která byla do té doby ve světě odhalena.[105]

Operace Newcaster fungovala na principu vytvoření fiktivní, ale důvěryhodné zpravodajské stránky NewsOnAir.org, kam útočníci vkládali články převzaté ze známých médií, například BBC či Reuters,[106] pod jmény fiktivních osob. V zájmu důvěryhodnosti vytvořili hackeři pro tyto osoby realistické profily na sociálních sítích, kde navazovali vztahy nejprve s příbuznými a přáteli obětí, později přímo se svými cílovými subjekty. Jedna osoba se snažila působit natolik důvěryhodně, že si vedla osobní blog o svém boji s depresí s názvem „Moje osamělost".[107] Některé osoby dokonce používaly jména nebo fotografie skutečných lidí. Jedna si říkala Sandra Maler, skutečná novinářka z Thompson Reuters ve Washingtonu, ačkoli používala fotky úplně jiné ženy.[108] Po vytvoření důvěry mezi obětí a útočníkem byly obětem zasílány odkazy, které infikovaly počítače škodlivým softwarem nebo je odkazovaly na webové stránky vyžadující přihlašovací údaje. V případě úspěchu došlo na straně oběti ke ztrátě a ukradení dat. V případě této operace není možné s určitostí říci, zda útočníci operovali samostatně nebo patřili pod vládní či jiné větší organizace (ačkoli vzhledem k složitosti operace to lze předpokládat), to ale nikterak neubírá na významu této hrozbě.[109] Nebyla ani odhalena jména těch, na které kampaň cílila, a není ani jasné, kolik cílů skutečně poskytlo své přihlašovací údaje nebo stáhlo škodlivý

---

[104] viz PERLROTH, Nicole. Cyberspionage Attacks Tied to Hackers in Iran. *The New York Times* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/

[105] viz FINKLE, Jim. Iranian hackers use fake Facebook accounts to spy on U.S., others. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/iran-hackers-idUSL1N0OE2CU20140529

[106] tamtéž

[107] viz PERLROTH, Nicole. Cyberspionage Attacks Tied to Hackers in Iran. *The New York Times* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/

[108] viz PIZZI, Michael. Iran hackers set up fake news site, personas to steal U.S. secrets. *Aljazeera America* [online]. 2014. [cit. 4.1.2023]. Dostupné z: http://america.aljazeera.com/articles/2014/5/29/iran-newscaster-hackers.html

[109] viz FINKLE, Jim. Iranian hackers use fake Facebook accounts to spy on U.S., others. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/iran-hackers-idUSL1N0OE2CU20140529

software. Lze nicméně předpokládat, že zcela bez úspěchu operace neproběhla.[110]

Zatímco experti iSight Partners nepotvrdili, zda měli hackeři vazby na íránskou vládu, analytici kybernetické bezpečnosti uvedli, že značné zpravodajské informace a zdroje, které jsou potřebné k provozování Newscasteru od roku 2011, poukazují na zapojení státu.[111]

3.3.2 Operace Cleaver

Počátkem roku 2014 publikovala americká softwarová společnost Cylance obsáhlou zprávu o operaci íránských hackerů, kterou pojmenovali Cleaver.[112] *„Írán byl vážně postižen v důsledku oslabující a extrémně pokročilé malwarové kampaně probíhající minimálně od roku 2009. Slavnými příklady těchto snah jsou průmyslové sabotáže prostřednictvím softwaru Stuxnet (2009 – 2010), a špionážních Duqu (2009 – 2011) nebo Flame (2012). Tyto kampaně byly zaměřeny na íránský jaderný program a operace související s ropou a zemním plynem. Stuxnet otevřel íránským autoritám oči, když je vystavil fyzickému ničení prostřednictvím elektronických prostředků*“, stojí v úvodu této zprávy zmiňujícím souvislost s malwarem Stuxnet, popsaným v předešlé kapitole.[113] O několik dnů později tuto zprávu potvrdil také americký Federální úřad pro vyšetřování (Federal Bureau of Investigation – FBI), rovněž hovořící o souvislosti s červem Stuxnet.[114]

Schopnosti zmíněné hackerské skupiny byly překvapující, dokázali totiž vstoupit do nejrůznějších infrastrukturních systémů v řadě zemí. Na seznamu cílů pochopitelně nechyběly Spojené státy s Izraelem, ale také Jižní Korea,

---

[110] viz PIZZI, Michael. Iran hackers set up fake news site, personas to steal U.S. secrets. *Aljazeera America* [online]. 2014. [cit. 4.1.2023]. Dostupné z: http://america.aljazeera.com/articles/2014/5/29/iran-newscaster-hackers.html

[111] tamtéž

[112] viz PAGANINI, Pierluigi. Operation Cleaver – Iranian hackers target industries worldwide. *SecurityAffairs.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://securityaffairs.co/30734/intelligence/operation-cleaver-iranian-hackers.html

[113] viz s. 6, McCLURE, Stuart. *Operation Cleaver*. Irvine, Cylcane, 2014. Dostupné z: https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf

[114] viz FINKLE, Jim. Iran hackers may target U.S. energy, defense firms, FBI warns. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/us-cybersecurity-iran-fbi-idUSKBN0JQ28Z20141213

Francie nebo třeba Německo. Útočníkům se v některých zemích dokonce podařilo získat vzdálený přístup do bezpečnostních systémů na letištích, což by jim hypoteticky umožnilo dostat na palubu nekontrolovaný materiál či osoby,[115] což je jen dalším příkladem provázanosti kyberprostoru s prostorem reálným. Seznam cílů identifikovaných výzkumníky z Cylance je velmi dlouhý a zahrnuje alespoň jeden jmenovitý vojenský subjekt v USA, intranet Navy Marine Corps (NMCI) a organizace v několika průmyslových odvětvích, jako je energetika a veřejné služby.[116]

Z výčtu zemí, proti kterým (resp. jejich institucím) byly operace vedeny, je patrné, že íránští hackeři se v tomto případě nesoustředili výhradně na své úhlavní nepřátele, ale rovněž na jejich spojence. Útok na Jižní Koreu by mohl posílit vztah mezi Íránem a Severní Koreou. V roce 2012 podepsal Írán dohodu o technologické kooperaci se Severní Koreou, což by jim mohlo umožnit kooperaci v otázkách jaderného programu i kybernetické bezpečnosti.[117]

Přestože v těchto případech je dokazování motivů nesnadné, odborníci z Cylance našli řadu domén použitých při různých útocích, které byly zaregistrovány na íránskou korporaci Tarh Andishan. Výzkumníci také zjistili, že ASN a síťové bloky jsou přímo propojeny s íránskými úřady, zatímco infrastrukturu využívanou k útokům provozuje íránský poskytovatel hostingu Netafraz.[118] *„Během intenzivního shromažďování zpravodajských informací za posledních 24 měsíců jsme pozorovali, že technické schopnosti týmu operace Cleaver se vyvíjejí rychleji, než jakékoli dříve pozorované íránské úsilí. Jak se schopnosti Íránu v oblasti kybernetického boje neustále vyvíjí, pravděpodobnost*

[115] viz PAGANINI, Pierluigi. Operation Cleaver – Iranian hackers target industries worldwide. *SecurityAffairs.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://securityaffairs.co/30734/intelligence/operation-cleaver-iranian-hackers.html
[116] viz PAGANINI, Pierluigi. Operation Cleaver – Iranian hackers target industries worldwide. *SecurityAffairs.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://securityaffairs.co/30734/intelligence/operation-cleaver-iranian-hackers.html
[117] viz McCLURE, Stuart. *Operation Cleaver*. Irvine, Cylcane, 2014. Dostupné z: https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf
[118] viz FINKLE, Jim. Iran hackers may target U.S. energy, defense firms, FBI warns. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/us-cybersecurity-iran-fbi-idUSKBN0JQ28Z20141213

útoku, který by mohl ovlivnit fyzický svět na národní nebo globální úrovni, rychle roste“, stojí dále ve zprávě Cylance.[119]

3.3.3 Shamoon

V srpnu roku 2012 zveřejnily společnosti Symantec, Kaspersky Labs a Seculert informace o novém malware nazvaným Shamoon, jehož název je odvozen z názvu složky ve spustitelném souboru. Spekuluje se, že jde o jméno jednoho z autorů malwaru, neboť Shamoon je ekvivalentem jména Simon v arabštině. Jednalo se o kybernetický útok na saudsko-arabskou ropnou společnost Aramco, která následně infikovala další ropné společnosti, jako například RasGas v Kataru, a taktéž nemocnice a univerzity.[120] Shamoon je malware typu botnet, který infikuje síť počítačů a následně ji řídí z jednoho centra. Po infikaci může dojít k DDoS útokům, spamu, ale i mazání disků (viz kap. 1).[121]

Právě mazání disků bylo úkolem Shamoona a svůj úkol splnil. Při první vlně útoků se útočníkům podařilo vymazat data z více než 30.000 počítačů.[122] Malware se rozšířil po síti a následně i mezi počítači obsluhovanými operačním systémem Windows. Útok Shamoonu nezpůsobil odstavení fyzického systému nebo explozi, ale i přesto došlo k ovlivnění ekonomických procesů a ke smazání významných dat společností. Samotné společnosti Aramco následně trvalo asi 14 dnů, než dokázala napravit způsobené škody.[123] K dalším útokům malwaru došlo v letech 2016, 2017 a 2018. Právě na základě opakovaného nasazení viru zpráva z roku 2020 předpokládá, že Írán ve vývoji Shamoona stále pokračuje

---

[119] viz McCLURE, Stuart. *Operation Cleaver*. Irvine, Cylcane, 2014. Dostupné z: https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf

[120] viz MACKENZIE, Heather. Shamoon Malware and SCADA Security – What are the Impacts? *TofinoSecurity.com* [online]. 2012. [cit. 4.1.2023]. Dostupné z: https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts

[121] viz LUTKEVICH, Ben. What is Botnet? *Techtarget* [online]. 2021. [cit. 29.10.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/botnet

[122] viz JEWKES, Stephen a Jim FINKLE. Shamoon computer virus variant is lead suspect in hack on oil firm Saipem. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/cyber-shamoon-idUSL1N1YH0QC

[123] viz MACKENZIE, Heather. Shamoon Malware and SCADA Security – What are the Impacts? *TofinoSecurity.com* [online]. 2012. [cit. 4.1.2023]. Dostupné z: https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts

s cílem vytvořit svůj vlastní Stuxnet schopný sabotovat petrochemické či obdobné závody.[124] Bezpečnostní experti se domnívají, že za útoky Shamoonu stáli lidé pracující jménem íránské vlády, což Teherán důrazně popírá. Podle výzkumníků byly v kódu nalezeny protiamerické snímky.[125]

3.3.4 Operace Ababil

Operace Ababil probíhala na podzim roku 2012, v době, kdy Spojené státy uvalily další sankce na íránské subjekty, mimo jiné íránskou centrální banku. Operace byla zaměřena na americké banky a další finanční instituce, využity přitom byly distribuované útoky odmítnutí služby k narušení platforem online bankovnictví. Přestože jsou útoky DDoS mezi experty považovány za relativně primitivní, operace Ababil byla účinně cílenou kampaní, která dočasně narušila některé obchodní funkce klíčového ekonomického pilíře USA a způsobila škody za desítky milionů dolarů. Navzdory tomu, že se k odpovědnosti přihlásila hacktivistická skupina Izz al-Din al-Qassam Cyber Fighters, dle Loudermilka byly téměř jistě schváleny íránskou vládou.[126] Podle New York Times ale neexistuje žádný přesvědčivý důkaz, že by tomu tak skutečně bylo. To koresponduje se skutečností, že ani američtí představitelé žádné podobné prohlášení veřejně neučinili, přestože dle CNN někteří toto přesvědčení neoficiálně vyjádřili, případně opatrněji hovořili o útocích iniciovaných státním činitelem, aniž by jej jmenovali.[127]

3.3.5 Další aktivity íránských hackerů

Přestože výše prezentovaný výčet není rozhodně komplexní a zahrnuje jen ty incidenty, které následovaly krátce po odhalení Stuxnetu,

---

[124] viz s. 7, KING FAISAL CENTER FOR RESEARCH AND ISLAMIC STUDIES. *Iran's Cyberattacks Capabilities.* Riyadh: KFCRIS, 2020.
[125] viz JEWKES, Stephen a Jim FINKLE. Shamoon computer virus variant is lead suspect in hack on oil firm Saipem. *Reutres.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/cyber-shamoon-idUSL1N1YH0QC
[126] LOUDERMILK, Micah. Iranian cyber actors are showing signs of battlespace preparation, so the United States should heed the lessons of past attacks and bolster its defensive posture. *The Washington Institute* [online]. 2019. [cit. 4.1.2023]. Dostupné z: https://www.washingtoninstitute.org/policy-analysis/iran-crisis-moves-cyberspace
[127] MOUNT, Mike. U.S. Officials believe Iran behind recent cyberattacks. CNN [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://edition.cnn.com/2012/10/15/world/iran-cyber/index.html

zřetelně ilustruje schopnosti íránských kybernetických útočníků a riziko, které představují pro Spojené státy.

Z dalších kybernetických útoků realizovaných íránskými útočníky lze jmenovat útok na přehradu Bowman Avenue nedaleko New Yorku v roce 2013, kde se útočníkům podařilo získat kontrolu nad protipovodňovými bariérami.[128] Dle dostupných zpráv se k útoku přihlásila íránská kybernetická skupina SOBH Cyber Jihad v roce 2015 s tím, že obdrželi varování „na státní úrovni", aby o útoku veřejně neinformovali,[129] aniž by toto varování blíže upřesnili. Není tak jasné, zda, příp. v jakém rozsahu, byl do akce zapojen Teherán. Několik amerických představitelů nicméně vydalo prohlášení, v nichž daný útok s Íránem coby předním světovým podporovatelem terorismu spojují.[130] V roce 2016 pak americké ministerstvo spravedlnosti oznámilo, že obvinilo sedm konkrétních hackerů, napojených na íránskou vládu, kteří za tímto útokem stáli, a zveřejnilo rovněž jejich jména. Jak uvádí The Washington Post,[131] bylo to poprvé, kdy Spojené státy obvinily státem sponzorované jednotlivce z hackerských útoků, jejichž cílem bylo narušení sítí klíčových amerických průmyslových odvětví. Nepředpokládá se přitom, že by Írán tyto osoby kdy vydal k trestnímu stíhání.

V roce 2018 Spojené státy obvinily a sankcionovaly devět Íránců a jednu íránskou společnost za pokus o průnik do stovek univerzit, firem a některých fragmentů americké vlády, včetně jejího hlavního energetického regulátora, a to jménem teheránské vlády. *„Hackeři nebyli obviněni z toho, že je přímo zaměstnává íránská vláda. Místo toho byli obviněni z kriminálního chování vedeného především prostřednictvím Institutu Mabna jménem Sboru islámských*

---

[128] viz PROKUPECZ, Shimon. Former official: Iranians hacked into New York dam. *CNN Politics* [online]. 2015. [cit. 5.1.2023]. Dostupné z: https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html

[129] viz ČESKÁ TELEVIZE. Útok íránských hackerů na přehradu v USA yvvolal diskuse o zastaralých systémech. *Česká televize* [online]. 2015. [cit. 5.1.2023]. Dostupné z: https://ct24.ceskatelevize.cz/svet/1647040-utok-iranskych-hackeru-na-prehradu-v-usa-vyvolal-diskuse-o-zastaralych-systemech

[130] viz PROKUPECZ, Shimon. Former official: Iranians hacked into New York dam. *CNN Politics* [online]. 2015. [cit. 5.1.2023]. Dostupné z: https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html

[131] NAKASHIMA, Ellen a Matt ZAPOTOSKY. U.S. charges Iran-linked hackers with targeting banks, N.Y. dam. *The Washington Post* [online]. 2016. [cit. 5.1.2023]. Dostupné z: https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html

revolučních gard, elitní vojenské síly určené k obraně íránské šíitské teokracie před vnitřními a vnějšími hrozbami“[132].

3.4 Spojené státy a kyberprostor

„Naše společnost a podpůrná kritická infrastruktura, od elektřiny po potrubí, je stále více digitální a zranitelnější vůči narušení nebo zničení prostřednictvím kybernetických útoků. … Spojené státy jakožto otevřená společnost mají jasný zájem o posílení norem, které zmírňují riziko kybernetických hrozeb a napomáhají stabilitě v kyberprostoru. Naším cílem je odrazení od kybernetických útoků jak ze strany státních, tak i nestátních aktérů, a s rozhodností a využitím všech dostupných prostředků budeme reagovat na nepřátelské činy v kybernetickém prostoru“,[133] deklarují Spojené státy svůj pevný postoj k obraně kybernetického prostoru ve své nejnovější Národní bezpečnostní strategii Spojených států z roku 2022. Citovaná pasáž nejenže podtrhuje závažnost zkoumané problematiky a deklaruje ochotu Spojených států bránit se kybernetickým útokům všemi dostupnými prostředky jako jakémukoli jinému vojenskému útoku, ale zdůrazňuje rovněž politiku otevřeného přístupu ke kyberprostoru a narůstající potřebu bránit zabezpečení kritické infrastruktury, jejíž značná část je ve Spojených státech vlastněna a provozována soukromým sektorem, což její ochranu znesnadňuje.[134]

Ochrana kyberprostoru se stala základní prioritou americké vlády (bez ohledu na to, zda je řeč o administrativě bývalých prezidentů Obamy a Trumpa či současného Bidena) a kybernetické bezpečnosti je věnováno mnoho vládních dokumentů. Mezi významné dokumenty patří zejména Mezinárodní strategie pro kyberprostor,[135] Národní kybernetická strategie,[136] Strategie kybernetické

---

[132] viz VOLZE, Dustina. U.S. charges sanctions Iranians for global cyber attacks on behalf of Tehran. *Reutres.com* [online]. 2018. [cit. 5.1.2023]. Dostupné z: https://www.reuters.com/article/us-usa-cyber-iran-idUSKBN1GZ22K

[133] viz s. 34, THE WHITE HOUSE. National Security Strategy. *The White House* [online]. 2022. [cit. 8.1.2023]. Dostupné z: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[134] viz THE WHITE HOUSE. FACT SHEET: Biden-Harris Administration Delivers on Strenghtheninh America’s Cybersecurity. *The White House* [online]. 2022. [cit. 8.1.2023]. Dostupné z: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/

[135] viz THE WHITE HOUSE. International Strategy for Cyberspace. *The White House* [online]. 2011. [cit. 8.1.2023]. Dostupné z:

bezpečnosti ministerstva vnitřní bezpečnosti,[137] či již zmíněná Národní bezpečnostní strategie Spojených států.[138]

Kybernetické bezpečnosti se v rámci Spojených států amerických věnuje několik vládních agentur. Mezi nejdůležitější subjekty, aktivní v této oblasti, patří:

- Armádní kybernetické velitelství (United States Cyber Command, CYBERCOM) představuje nejvyšší velení kybernetických jednotek a je začleněno v rámci Strategického velení (Strategic Command, STRATCOM) Ministerstva obrany USA. Zahrnuje jednotky námořnictva, pozemních a leteckých sil.
- Centrum kybernetické kriminality při Ministerstvu obrany (Department of Defence Cyber Crime Center, DoD CCC, DC3)
- Národní bezpečnostní agentura (National Security Agency, NSA), Federální úřad pro vyšetřování (Federal Bureau of Investigation, FBI) a Ústřední zpravodajská služba (Central Intelligence Agency, CIA). Jejich role spočívá hlavně ve shromažďování informací, nikoli v účasti na kybernetických operacích.
- Ministerstvo vnitřní bezpečnosti (Department of Homeland Security - DHS) má za úkol chránit sítě a systémy federální vlády.

3.5 Irán a kyberprostor

Již dříve v této práci bylo konstatováno, že autority na celém světě i široká veřejnost si již uvědomují, že kyberprostor je dnes třeba chápat jako regulérní válečnou doménu se svými vlastními specifiky. Na jedné straně může poskytovat významný manévrovací prostor a prostředek konkurenční výhody, na straně druhé může také představovat slabé místo, které mohou nepřátelské elementy

---

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[136] viz THE WHITE HOUSE. National Cyber Strategy. *The White House* [online]. 2018. [cit. 8.1.2023]. Dostupné z: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[137] viz U.S. DEPARTMENT OF HOMELAND SECURITY. Cybersecurity Strategy. *U.S. Department of Homeland Security* [online]. 2018. [cit. 8.1.2023]. Dostupné z: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[138] viz THE WHITE HOUSE. National Security Strategy. *The White House* [online]. 2022. [cit. 8.1.2023]. Dostupné z: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

využít k vyřazení informačních systémů nebo dokonce způsobení fyzické škody v oblasti kritické infrastruktury řízené průmyslovými řídicími systémy. Útok Stuxnetu směřovaný proti íránskému jadernému programu poskytl tuto zkušenost také Íránu.

V oblasti obrany Írán pracuje na dosažení dvou hlavních cílů v kyberprostoru. Za prvé se zaměřuje na efektivní, komplexní, pokročilý technologický ochranný systém na obranu kritických infrastruktur a citlivých dat proti kybernetickým útokům, jakým je Stuxnet. Za druhé, Írán se snaží omezit a zmařit kyberprostorové aktivity domácích opozičních stran a odpůrců režimu, pro které je kyberprostor důležitou komunikační platformou pro šíření informací a organizování protivládních aktivit. Režim navíc doufá, že v rámci kyberprostoru zabrání pronikání západních myšlenek a informací, které jsou v rozporu s jeho zájmy. Na útočné frontě vnímají íránští představitelé kyberprostor jako jeden z významných nástrojů asymetrického vedení boje, podobně jako zjevnější asymetrické taktiky, jakými je terorismus a partyzánská válka. Tedy jako účinný nástroj způsobující značné poškození nepříteli s vojenskou nebo geostrategickou převahou.[139]

Írán začal se strategickým budováním svých národních kybernetických sil přibližně v roce 2003. V rámci relevantních ministerstev tak vznikaly nové organizační struktury věnující se kybernetické bezpečnosti. Snahou Íránu bylo vytvoření hierarchického a zároveň různorodého organizačního systému. V roce 2012 zde byla založena kybernetická jednotka zvaná Nejvyšší rada pro kyberprostor (Supreme Council of Cyberspace – SCC), která má neomezenou kontrolu nad informacemi na internetu v zemi, jejich následnou regulaci a určuje národní strategie a politiky v kybernetickém prostoru.[140] V čele Rady stojí íránský prezident a jejími členy jsou vysocí vládní představitelé a další, včetně vysokého velitele Revoluční gardy, ministrů vědy, komunikace a kultury, šéfa policie a prezidenta islámské propagandistické organizace.[141] Významnou centrální organizací defenzivní povahy je Velitelství obrany v kyberprostoru, spadající pod

[139] viz s. 83, SIBONI, Gabi a Sami KRONENFELD. *Cyberspace and National Security*. Tel Aviv: Institute for National Security Studies, 2013. ISBN 978-965-7425-51-0.
[140] viz SMALL MEDIA. Iranian Internet Infrastructure and Policy Report. *Smallmedia* [online]. 2014. [cit. 7.1.2023]. Dostupné z: https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf
[141] tamtéž

generální štáb ozbrojených sil. Jeho hlavním cílem je rozvoj bezpečnostní strategie pro státní instituce proti kybernetickým hrozbám. Podobně obrannou složkou je rovněž Centrum pro informační bezpečnost, známé jako MAHER, které je zodpovědné za aktivaci reakcí na bezpečnostní hrozby a kybernetické útoky.[142]

Úkolem jiných íránských organizací působících v kyberprostoru je prosazování a kontrola vnitrostátních kybernetických aktivit, zejména těch, které jsou v rozporu se zájmy režimu. Jmenovat lze například Výbor pro identifikaci nežádoucích webových stránek, jehož účelem je identifikace těch stránek, jejichž obsah a činnost jsou neslučitelné se stanovisky režimu, a tyto stránky blokovat; či policejní jednotku FATA. Mezi aktivity FATA patří snaha zastavit využívání VPN, díky kterým se dařilo obcházet internetovou cenzuru. Dále například zatčení Sattara Beheshtiho, který kritizoval íránskou vládu na svém blogu, a následně byl nalezen mrtev ve své cele. Je možné, že byl mučen až k smrti policejními představiteli. Díky tomuto případu se dostala FATA do problému a následně byl její šéf propuštěn. Poté se FATA zaměřila spíše na finanční kybernetické prohřešky, podvody a sledování se přesunulo pod Íránskou revoluční gardu a Nejvyšší radu pro kyberprostor.[143]

Pokud jde o útočné schopnosti Íránců, obrázek je v tomto ohledu méně zřetelný, neboť se jedná o strategické informace podléhající určitému utajení. O schopnostech i motivaci íránských autorit klamat a utajovat informace strategické povahy není pochyb, příkladem budiž četné nesrovnalosti mezi zjištěním expertů IAEA a tvrzením íránských představitelů ve věci jejich jaderného programu, stejně jako některé dříve popisované kybernetické incidenty, které jsou v západní společnosti považovány za aktivity přinejmenším posvěcené íránskou vládou, ačkoli tato jakékoli zapojení kategoricky odmítá. Významnou roli zde hrají Íránské islámské revoluční gardy. Analýza pocházející

[142] viz s. 88, SIBONI, Gabi a Sami KRONENFELD. *Cyberspace and National Security*. Tel Aviv: Institute for National Security Studies, 2013. ISBN 978-965-7425-51-0.
[143] viz SMALL MEDIA. Iranian Internet Infrastructure and Policy Report. *Smallmedia* [online]. 2013. [cit. 7.1.2023]. Dostupné z: https://smallmedia.org.uk/sites/default/files/u8/IIIPSepOct.pdf

z roku 2008[144] odhaduje, že revoluční gardy Íránu zaměstnávaly asi 2 400 pracovníků kybernetických jednotek, a dle úrovně jejich schopností je řadí mezi nejlepší pětici světa. Schopnostmi, které jsou v tomto materiálu íránským revolučním gardám připisovány, jsou:

- vývoj infikovaného softwaru vložením škodlivého kódu do padělaného softwaru;
- schopnosti blokovat komunikační a wifi sítě;
- vývoj škodlivých kódů schopných reprodukce;
- vývoj nástrojů pro pronikání do sítí a počítačů nepřítele schopných shromažďovat a předávat důležité informace.

Revoluční gardy také vytvářejí systém elektronického boje schopný blokovat radary či jakoukoli jinou komunikaci. Kromě kyberprostorových bojových jednotek revolučních gard existují důkazy spojující revoluční gardy a skupiny íránských hackerů, kteří jsou aktivní proti domácím i globálním nepřátelům režimu. Použití outsourcingu umožňuje revolučním gardám a Íránu udržovat si odstup a vyvrátit jakákoli obvinění z íránského zapojení do kybernetických útoků. Některé tyto skupiny spolu soupeří, jindy naopak spolupracují na dosažení společného cíle.[145] Experti identifikovali jednu skupinu íránských hackerů spojenou s revolučními gardami – Ashiyane, jejíž členové jsou motivováni ideologií podporující íránský režim a revoluci, a kteří míří svými útoky na nepřátele režimu, a to jak nepřátele zvenčí, tak i domácí. Skupina mimo jiné pořádala fórum s názvem War Games, které organizovalo hackerské soutěže, jejichž cíle byly americké infrastrukturní společnosti.[146]

O zodpovědnějším přístupu iránských představitelů na poli kybernetické bezpečnosti vyvolaném červem Stuxnet mohou vypovídat i vybrané finanční ukazatele, zejména pokud jde o výdaje na kybernetickou bezpečnost země. Ty jsou zachyceny v grafu 1.

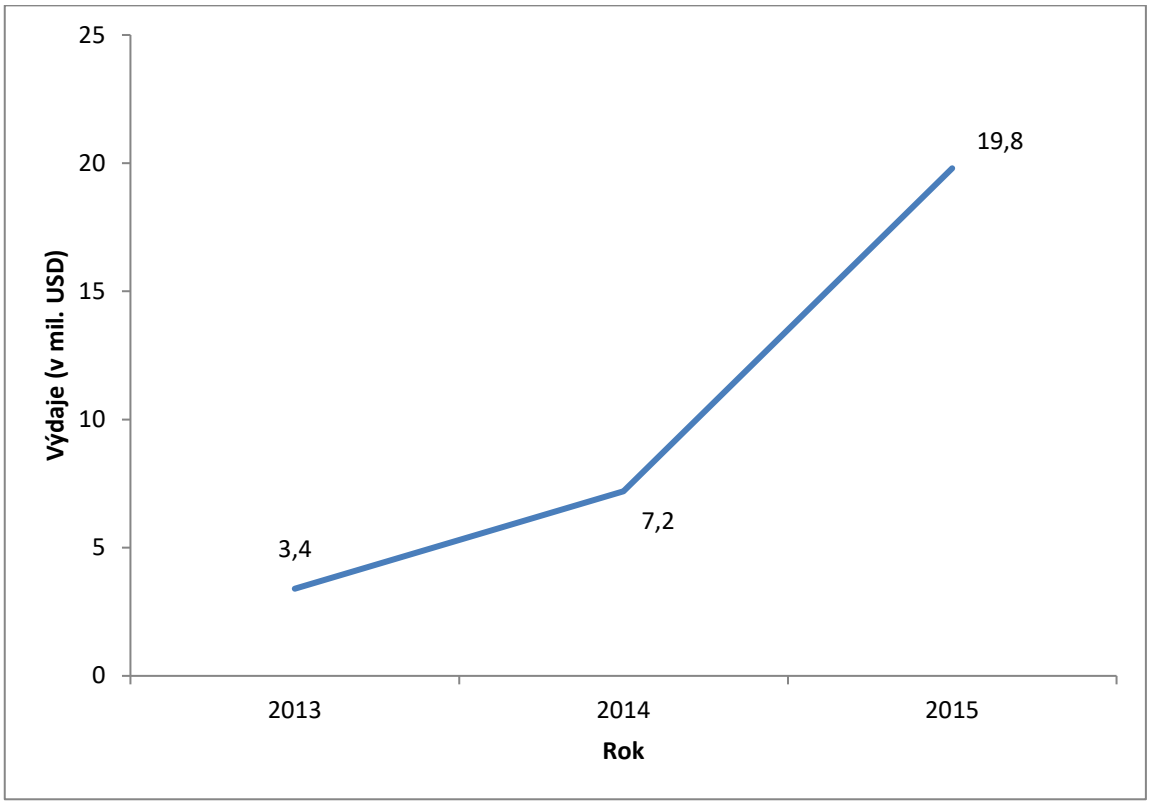
---

[144] viz COLEMAN, Kevin. Iranian Cyber Warfare Threat Assessment. *Military.com* online]. 2008. [cit. 7.1.2023]. Dostupné z: https://www.military.com/defensetech/2008/09/23/iranian-cyber-warfare-threat-assessment

[145] viz s. 11, KING FAISAL CENTER FOR RESEARCH AND ISLAMIC STUDIES. *Iran's Cyberattacks Capabilities.* Riyadh: KFCRIS, 2020.

[146] viz s. 90, SIBONI, Gabi a Sami KRONENFELD. *Cyberspace and National Security*. Tel Aviv: Institute for National Security Studies, 2013. ISBN 978-965-7425-51-0.

Graf 1: Íránský rozpočet na kybernetickou bezpečnost v letech 2013 – 2016 (v mil. USD)[147]



Na tomto místě je nutno podotknout, že období sledované v grafu 1 počíná rokem 2013, kdy v Íránu nastoupil k moci prezident Rúhání, a nereflektuje tedy období následující bezprostředně po útoku malwaru Stuxnet. Tento nesoulad vychází ze skutečnosti, že Írán začal zveřejnovat údaje o svých výdajích na kybernetickou bezpečnost až s nástupem prezidenta Rúháního.[148] Údaje z předešlých let tedy chybí, dostupné jsou pouze odhady, v nichž lze nalézt často signifikantní rozdíly, či jsou uváděny v kontextu s jinými výdaji (například celkové výdaje ministerstva ICT (The Ministry of Information and Communications Technology – ICT). Přesto i tyto omezené údaje poskytují alespoň částečný obrázek toho, nakolik se změnil přístup Íránu k operacím v kyberprostoru po útoku Stuxnetu. Z grafu 1 je patrný růst výdajů na

[147] viz s. 147 PISSANIDIS, Nikolaos, Henry, RÕGAS a Matthijs VEENENDAAL. *2016 8th International Conference on Cyber Conflict: Cyber Power*. Tallinn: NATO CCD COE Publications, 2016. ISBN 978-9949-9544-9-0.
[148] viz s. 146 PISSANIDIS, Nikolaos, Henry, RÕGAS a Matthijs VEENENDAAL. *2016 8th International Conference on Cyber Conflict: Cyber Power*. Tallinn: NATO CCD COE Publications, 2016. ISBN 978-9949-9544-9-0.

kybernetickou bezpečnost země, který během pouhých dvou let dosáhl hodnoty bezmála 600 %.

Závěr

Kybernetická válka je relativně nový fenomén, který se do popředí zájmu dostává teprve v posledních několika dekádách. Lze ho považovat za přirozený důsledek dynamického vývoje technologických prostředků, i změn, které tyto prostředky přinášejí do naší společnosti. Tyto skutečnosti však nikterak neubírají na významu tématu či jeho složitosti, ba naopak. Pro jeho plné pochopení je nutné hlouběji proniknout nejen do problematiky kybernetické bezpečnosti, ale také bezpečnosti mezinárodní.

Přestože rámec zkoumané problematiky je velmi široký a informace prezentované v této práci nejsou (a ani nemohou být) všezahrnující, považoval autor za důležité úvodem definovat pojmy, jejichž pochopení je pro studium problematiky nezbytné. V rámci teoretických vstupů autor rovněž přibližuje vývoj posledního půlstoletí z několika perspektiv – pohledem obecného technologického vývoje, reakce teorie mezinárodních vztahů na tento vývoj, a konečně také perspektivou vojenskou. To poskytuje vysvětlení, proč na počátku 21. století Spojené státy i Severoatlantická aliance (ale i další subjekty) uznaly kybernetický prostor jako novou doménu, které je při obraně nutné věnovat stejnou pozornost, jako obraně ve vzduchu, na zemi i na moři (případně ve vesmíru). V souladu s tím byl věnován prostor také teorii rozšířeného pojetí bezpečnosti kodaňské školy, v rámci které bylo pět tradičních sektorů bezpečnosti rozšířeno právě o kybernetický prostor. Akceptace tohoto předpokladu nejenže vysvětluje výše uvedené, ale odpovídá také lépe současným podmínkám a podtrhuje tak význam daného tématu. Jestliže relativně malá skupina útočníků dokáže pomocí výpočetní techniky nefyzicky proniknout do přísně střeženého podzemního závodu uprostřed pouště, k tomu odpojeného od internetu, a způsobit zde fyzické škody nesmírného rozsahu, nelze význam kybernetických útoků bagatelizovat. Oprávněně si lze klást otázku, jak daleko je lidstvo od toho, aby podobným způsobem zabíjelo ve velkém podobně, jako zbraně hromadného ničení.

Případová studie byla věnována konkrétnímu, výše nastíněnému incidentu, kdy byl prostřednictvím nesmírně sofistikovaného malwaru Stuxnet

napaden jaderný závod v íránském Natanzu. Příčinu útoku lze spatřovat v samotné existenci těchto, mezinárodnímu dohledu se vymykajících zařízení na íránském území, vyvolávajících obavy, že Írán usiluje o vývoj jaderné zbraně. Incident byl charakteristický tím, že představoval případ útoku z kybernetického prostředí na fyzická zařízení, která dokázal reálně poškodit. To vše zcela nepozorovaně, bez významnějších vedlejších škod a s podobným výsledkem, jaký by přinesla pozemní invaze či spíše letecký úder na tato zařízení. Experti zabývající se kybernetickou bezpečností řadí Stuxnet k nejpropracovanějším virům vůbec a považují jej za zřetelnou demonstraci toho, jak může válčení budoucnosti vypadat. Aniž by se k útoku některý stát oficiálně přiznal, odborníci se veskrze shodují, že se jednalo o společnou americko-izraelskou operaci. V podobném duchu se vyjádřili i mnozí představitelé amerických tajných služeb, někteří autoři pak identifikovali konkrétní tým programátorů Stuxnetu nebo naopak popisují detaily z jednání o nasazení zbraně s tehdejším americkým prezidentem Bushem. Na základě studovaných materiálů se autor k tomuto názoru přiklání, neboť neshledal žádné důvody jej jakkoli zpochybňovat. Podobně je tomu i v případě později objeveného viru Duqu, ačkoli tento incident nebyl podrobněji studován.

Studována naopak byla reakce Íránu na odhalení Stuxnetu. Přestože Írán, coby jeden z největších státních podporovatelů terorismu na světě inklinující k metodám asymetrického válčení, začal s budováním svých kybernetických kapacit již v roce 2003, po lekci uštědřené nasazením Stuxnetu je patrné výrazné navýšení tohoto úsilí. O tom vypovídá zřízení Nejvyšší rady pro kyberprostor (SCC) a řady dalších íránských organizací zabývajících se touto problematikou, ale částečně také enormní nárůst íránských výdajů na kybernetickou bezpečnost nebo zvýšená aktivita íránských hackerů v kyberprostoru. A koneckonců také zprávy, které řadí schopnosti íránských kybernetických sil mezi nejlepší pětici světa. Z hlediska zkoumané problematiky jsou podstatné především útočné schopnosti Íránu v kyberprostoru, nicméně v tomto ohledu není obraz zcela jasný. Mnozí experti se na základě řady indicií domnívají, že Írán v těch otázkách často využívá outsourcingu, který poskytuje režimu určitý odstup a argument proti případným obviněním ze zapojení do kybernetických útoků. Vezmeme-li v potaz vazby Teheránu na teroristické či jiné

zločinecké organizace a jeho vztah k asymetrickému válčení, mají takové úvahy své opodstatnění, ačkoli přímé důkazy chybí. Pokud jde o konkrétní útoky, zaujme nasazení viru Shamoon, připisovaného Íránu, ačkoli v tomto ohledu útok nesměřoval na Spojené státy, nýbrž primárně na saudskoarabskou společnost Aramco. Z hlediska propracovanosti zaujme také operace Newcaster, namířená proti americkým vojenským dodavatelům, kongresmanům a jiným významným osobám, nicméně v tomto případě nelze s jistotou říci, nakolik se na útoku podílela íránská vláda. Svým rozsahem je zajímavá také operace Cleaver, v rámci které byly nabourány infrastrukturní systémy Spojených států a jejich spojenců. Ačkoli tyto útoky nezpůsobily větší škody, řada z nich byla úspěšná s potenciálem působit škodu na majetku nebo dokonce na zdraví lidí. Útoky zahrnuté pod operaci Cleaver bezpečnostní experti i představitelé tajných služeb považují za íránskou odpověď na Stuxnet. Podobně je tomu i v případě operace Ababil, namířené proti americkým finančním institucím, či útoku na přehradu Bowman Avenue v roce 2013. Z posledně jmenovaného byli dokonce obviněni konkrétní útočníci napojení na íránskou vládu.

V rámci diplomové práce byla testována hypotéza, že mezi Spojenými státy a Íránem probíhá plnohodnotná kybernetická válka. Na základě studovaných materiálů si na tomto místě autor dovoluje tvrdit, že zkoumaný incident lze považovat za kybernetickou válku. Incident naplňuje všechny prvky státocentrické definice, neboť za „jakékoli jednání státu“ lze označit jak útok kooperovaný s třetím aktérem (spolupráce Spojených států s Izraelem) tak rovněž outsourcing v podání Íránu. Definice Výkladového slovníku kybernetické bezpečnosti dále hovoří o „souvisejících a vzájemně vyvolaných organizovaných útocích a protiútocích“, přičemž souvislost mezi výše vzpomínanými útoky lze nalézt rovněž. Pokud se týká samotného pojmu kybernetický útok, i přísnějšímu vymezení dle Tallinnského manuálu 2.0 tyto útoky odpovídají, neboť (přinejmenším některé z nich) prokázaly schopnost působit škodu na majetku, potenciálně i na zdraví lidí. Hypotéza proto byla přijata.

Seznam použité literatury

Monografie

1. BROŽ, Ivan. *Husajn kontra Chomejní: irácko-íránská válka1980-1988*. Praha: Epocha, 2007. ISBN 978-80-87027-12-7.
2. BUZAN, Barry, Ole WAEVER a Jaap DE WILDE. *Bezpečnost: Nový rámec pro analýzu*. Brno: Centrum strategických studií, 2005. ISBN 80-903333-6-2.
3. CIRINCIONE, Joseph. *Repairing the Regime: Preventing the Spread of Weapons of Mass Destruction*. New York, London: Routledge, 2000. ISBN 0-415-92595-9.
4. CLARKE, Richard A. a Robert K. KNAKE. *The Next Threat to National Security and What to Do About IT*. New York: HarperCollins, 2010. ISBN 978-0-06-199239-1.
5. CORNISH, Paul et al. *On Cyber Warfare*. London: The Royal Institute of International Affairs, 2010. ISBN 978-1-86203-243-9.
6. CVRKAL, Zdeněk. *Írán – stručná historie státu*. Praha: Libri, 2007. ISBN 978-80-7277-337-4.
7. FUČÍK, Jakub. *Vývoj konceptu současné revoluce ve vojenských záležitostech*. Brno, 2017. Disertační práce. Masarykova Univerzita, Fakulta sociálních studií, Katedra mezinárodních vztahů a evropských studií. Vedoucí práce doc. PhDr. Zdeněk Kříž, Ph.D.
8. GRAY, Colin S. *Strategy and History: Essays on Theory and Practice*. London: Routledge, 2006. ISBN 0-203-96490-X.
9. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 2. akt. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.
10. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Granda, 2007. ISBN 978-80-247-1561-2.
11. KAPLAN, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon, 2017. ISBN 978-1-4767-6326-2.

12. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
13. KRAUS, Josef. *Íránský státní terorismus: Od Chomejního po Ahmadínežáda*. Brno: Centrum pro studium demokracie a kultury, 2014. ISBN 978-80-7325-342-4.
14. KŘÍŽ, Zdeněk, et al. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. Ostrava: Jagello, 2015. ISBN 978-80-904850-2-0.
15. MAŘÍK, Vladimír. *Průmysl 4.0: Výzva pro Českou republiku*. Praha: Management Press, 2016. ISBN 978-80-7261-440-0.
16. McCULLOH, Timothy B. a Richard B. JOHNSON. *Hybrid Warfare*. Florida: MacDill Air Force Base, 2013. ISBN 978-1-933749-77-8.
17. SCHMITT, Michael N. *Tallin Manual 2.0: On the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. ISBN 978-1-107-17722-2.
18. SIBONI, Gabi a Sami KRONENFELD. *Cyberspace and National Security*. Tel Aviv: Institute for National Security Studies, 2013. ISBN 978-965-7425-51-0.
19. SOLIS, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*. 2nd ed. Cambridge: Cambridge University Press, 2016. ISBN 978-1-107-13560-4.
20. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
21. WAISOVÁ, Šárka. *Bezpečnost - vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-21-0.
22. ZETTER, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, Crown, 2014. ISBN 978-0-7704-3618-6.

Webové stránky a elektronické zdroje

23. ARQUILLA, John a David RONFELDT. Cyberwar is Coming! *Rand Corporation* [online]. 1993. [cit. 15.10.2022]. Dostupné z: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

24. BALDWIN, David A. The Concept of Security. *Review of International Studies* [online]. 1997, roč. 23, č. 1. [cit. 16.10.2022]. ISSN 0260-2105. Dostupné z: https://www.cambridge.org/core/journals/review-of-international-studies/article/abs/concept-of-security/67188B6038200A97C0B0A370FDC9D6B8
25. ČESKÁ TELEVIZE. Útok íránských hackerů na přehradu v USA vyvolal diskuse o zastaralých systémech. *Česká televize* [online]. 2015. [cit. 5.1.2023]. Dostupné z: https://ct24.ceskatelevize.cz/svet/1647040-utok-iranskych-hackeru-na-prehradu-v-usa-vyvolal-diskuse-o-zastaralych-systemech
26. ČESKÁ TELEVIZE. Ruští špioni vedou v ČR informační válku, čínští usilují o vliv, říká zpráva tajné služby. *Česká televize* [online]. 2016. [cit. 14.11.2022]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/1893620-v-cesku-loni-nejvice-pusobili-spioni-z-ruska-a-ciny
27. COLEMAN, Kevin. Iranian Cyber Warfare Threat Assessment. *MIlitary.com* [online]. 2008. [cit. 7.1.2023]. Dostupné z: https://www.military.com/defensetech/2008/09/23/iranian-cyber-warfare-threat-assessment
28. DAVENPORT, Kelsey. Timeline of Nuclear Dimplomacy with Iran. *Arms Control Association* [online]. 2022. [cit. 3.1.2023]. Dostupné z: https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran
29. DEPARTMENT OF HOMELAND SECURITY. Cyber Threat Source Descriptions. *CISA* [online]. 2005. [cit. 15.11.2022]. Dostupné z: https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions
30. DEWAR, Robert S. *Active Cyber Defense*. Zürich: Center of Security Studies, 2017. Dostupné z: https://www.research-collection.ethz.ch/handle/20.500.11850/181743
31. ERBEN, Lukáš. Příchod hackerů: příběh Stuxnet. *Root.cz* [online]. 2014. [cit. 3.1.2023]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

32. ERBEN, Lukáš. Příchod hackerů: operace Olympijské hry. *Root.cz* [online]. 2014. [cit. 3.1.2023]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-operace-olympijske-hry/
33. FELIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany v rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. 2017, roč. 26, č. 3. [cit. 18.10.2022]. ISSN 2336-2995. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/vystavba-ozbrojenych-sil/aktualni-ukoly-kyberneticke
34. FINKLE, Jim. Iranian hackers use fake Facebook accounts to spy on U.S., others. *Reuters.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/iran-hackers-idUSL1N0OE2CU20140529
35. FINKLE, Jim. Exclusive: Iran hackers may target U.S. enegry, defense firm, FBI warns. *Reuters.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/us-cybersecurity-iran-fbi-idUSKBN0JQ28Z20141213
36. HANSEN, Lene a Helen NISSENBAUM. Digital Disaster, Cyber Security, and the Copenhagen school. *International Studies Quarterly* [online]. 2009, roč. 53, č. 4. [cit. 16.10.2022]. ISSN 1468-2478. Dostupné z: https://is.muni.cz/el/fss/podzim2020/IREb1007/84255154/11._digital_disaster.pdf
37. NAKASHIMA, Ellen a Matt ZAPOTOSKY. U.S. charges Iran-linked hackers with targeting banks, N.Y. dam. *The Washington Post* [online]. 2016. [cit. 5.1.2023]. Dostupné z: https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html
38. NTI. Iran Nuclear Overview. *NTI* [online]. 2020. [cit. 1.1.2023]. Dostupné z: https://www.nti.org/analysis/articles/iran-nuclear/
39. PAGANINI, Pierluigi. Operation Cleaver – Iranian hackers target industries worldwide. *SecurityAffairs.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://securityaffairs.co/30734/intelligence/operation-cleaver-iranian-hackers.html

40. JAHANPOUR, Farhang. Chronology of Iran's Nuclear Programme, 1957-2007. *Oxford Research Group* [online]. 2007. [cit. 29.12.2022]. Dostupné z: https://www.oxfordresearchgroup.org.uk/work/middle_east/iranchronology.php
41. JEWKES, Stephen a Jim FINKLE. Shamoon computer virus variant is lead suspect in hack on oil firm Saipem. *Reuters.com* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://www.reuters.com/article/cyber-shamoon-idUSL1N1YH0QC
42. KLEINROCK, Leonard. An Early History of the Internet. *IEEE Communications Magazine* [online]. 2010, roč. 48, č. 8. [cit. 16.11.2022]. ISSN 1558-1896. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5534584
43. KUBEŠA, Milan. Vojenské klamání v informačním věku. *Vojenské rozhledy* [online]. 2013, roč. 22 (54), č. 1. [cit. 17.10.2022]. ISSN 2010-3292. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/vojenske-klamani-v-informacnim-veku
44. LOUDERMILK, Micah. Iranian cyber actors are showing signs of battlespace preparation, so the United States should heed the lessons of past attacks and bolster its defensive posture. *The Washington Institute* [online]. 2019. [cit. 4.1.2023]. Dostupné z: https://www.washingtoninstitute.org/policy-analysis/iran-crisis-moves-cyberspace
45. LUTKEVICH, Ben. What is Botnet? *Techtarget* [online]. 2021. [cit. 29.10.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/botnet
46. MACKENZIE, Heather. Shamoon Malware and SCADA Security – What are the Impacts? *TofinoSecurity.com* [online]. 2012. [cit. 4.1.2023]. Dostupné z: https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts
47. McCLURE, Stuart. *Operation Cleaver*. Irvine, Cylcane, 2014. Dostupné z: https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf

48. MINIWATTS MARKETING GROUP. World Internet Users Statistics and 2022 World Population Stats. *Internet World Stats* [online]. 2022. [cit. 16.10.2022]. Dostupné z: https://www.internetworldstats.com/stats.htm
49. MOUNT, Mike. U.S. Officials believe Iran behind recent cyberattacks. *CNN* [online]. 2012. [cit. 4.1.2023]. Dostupné z: https://edition.cnn.com/2012/10/15/world/iran-cyber/index.html
50. NATO. Cyber Defence. *North Atlantic Treaty Organization* [online]. 2022. Dostupné z: https://www.nato.int/cps/en/natohq/topics_78170.htm
51. NYE, Joseph S. Is Military Power Becoming Obsolete? *Project Syndicate* [online]. 2010. [cit. 13.11.2022]. Dostupné z: https://www.project-syndicate.org/commentary/is-military-power-becoming-obsolete-2010-01
52. NYE, Joseph S. The Information Revolution Gets Political. *Belfer Center for Science and International Affairs* [online]. 2013. [cit. 13.11.2022]. Dostupné z: https://www.belfercenter.org/publication/information-revolution-gets-political
53. OBAMA, Barack. Remarks by the President at the Acceptance of the Nobel Peace Prize. *The White House* [online]. 2009. [cit. 13.10.2022]. Dostupné z: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize
54. OTTIS, Rain a Peeter LORENTS. Cyberspace: Definition and Implications. *Cooperative Cyber Defence Centre of Excellence* [online]. 2012. [cit. 16.10.2022]. Dostupné z: https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf
55. OWENS, William A., Kenneth W. DAM a Herbert S. LIN. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. *National Academies.* [online]. 2013. [cit. 18.10.2022]. Dostupné z: https://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf
56. PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. *Bezpečnostní teorie a praxe* [online]. 2015, č. 3. [cit. 19.10.2022].

Dostupné z: https://is.muni.cz/el/fss/podzim2018/BSS469/um/Role_statu_sken.pdf

57. PERLROTH, Nicole. Cyberspionage Attacks Tied to Hackers in Iran. *The New York Times* [online]. 2014. [cit. 4.1.2023]. Dostupné z: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/
58. PIZZI, Michael. Iran hackers set up fake news site, personas to steal U.S. secrets. *Aljazeera America* [online]. 2014. [cit. 4.1.2023]. Dostupné z: http://america.aljazeera.com/articles/2014/5/29/iran-newscaster-hackers.html
59. PROKUPECZ, Shimon. Former official: Iranians hacked into New York dam. *CNN Politics* [online]. 2015. [cit. 5.1.2023]. Dostupné z: https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html
60. SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012. [cit. 3.1.2023]. Dostupné z: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
61. SHACKELFORD, Scott J. Towards Cyber Peace: Managing Cyber Attacks Through Polycentric Governance. *American University Law Review* [online]. 2013, roč. 62, č. 5. [cit. 17.11.2022]. Dostupné z: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1888&context=aulr
62. SMALL MEDIA. Iranian Internet Infrastructure and Policy Report. *Smallmedia* [online]. 2013. [cit. 7.1.2023]. Dostupné z: https://smallmedia.org.uk/sites/default/files/u8/IIIPSepOct.pdf
63. SMALL MEDIA. Iranian Internet Infrastructure and Policy Report. *Smallmedia* [online]. 2014. [cit. 7.1.2023]. Dostupné z: https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf
64. ŠEVEČEK, Martin. Íránský jaderný program – vznik sankcí, současnost a budoucnost. *OENERGETICE.CZ* online]. 2016. [cit. 1.1.2023]. Dostupné z: https://oenergetice.cz/ropa/iransky-jaderny-program-je-pod-kontrolou-co-nas-ceka-dal

65. THE WHITE HOUSE. National Security Strategy. *The White House* [online]. 2010. [cit. 17.10.2022]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
66. THE WHITE HOUSE. International Strategy for Cyberspace. *The White House* [online]. 2011. [cit. 8.1.2023]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
67. THE WHITE HOUSE. National Cyber Strategy. *The White House* [online]. 2018. [cit. 8.1.2023]. Dostupné z: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
68. THE WHITE HOUSE. National Security Strategy. *The White House* [online]. 2022. [cit. 8.1.2023]. Dostupné z: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
69. THE WHITE HOUSE. FACT SHEET: Biden-Harris Administration Delivers on Strenghthening America's Cybersecurity. *The White House* [online]. 2022. [cit. 8.1.2023]. Dostupné z: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/
70. U.S. DEPARTMENT OF HOMELAND SECURITY. Cybersecurity Strategy. *U.S. Department of Homeland Security* [online]. 2018. [cit. 8.1.2023]. Dostupné z: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
71. VOLZE, Dustina. U.S. charges, sanctions Iranians for global cyber attacks on behalf of Tehran. *Reuters.com* [online]. 2018. [cit. 5.1.2023]. Dostupné z: https://www.reuters.com/article/us-usa-cyber-iran-idUSKBN1GZ22K
72. WAISOVÁ, Šárka. Od národní bezpečnosti k mezinárodní bezpečnosti. *Global Politicis: časopis pro politiku a mezinárodní vztahy* [online]. 2004, č. 3. [cit. 15.10.2022]. ISSN 1213-7685. Dostupné z: https://mv.iir.cz/article/view/124/pdf