MASARYKOVA UNIVERZITA

Fakulta sociálních studií

Katedra politologie

Bezpečnostní a strategická studia

Magisterská diplomová práce

Kybernetické konflikty v postsovětském prostoru

Václav Borovička, 325902

Brno, Jaro 2015

Prohlašuji, že jsem diplomovou práci na téma „*Kybernetické konflikty v postsovětském prostoru“* vypracoval samostatně a použil jen zdroje uvedené v seznamu literatury.

V Brně 20. 5. 2015

.....

Václav Borovička

Rád bych na tomto místě poděkoval Mgr. Tomáši Šmídovi, Ph.D. za vedení mé diplomové práce, za poskytnutí cenných rad, odborných názorů, a zejména pak za vstřícnost a trpělivost, kterou se mnou nejen při vypracovávání této diplomové práce měl.

Dále bych rád poděkoval svým nadřízeným a kolegům za podporu, kterou mi při psaní práce poskytovali.

V neposlední řadě chci poděkovat svým rodičům, rodině a přátelům za veškerou podporu, kterou na mě v průběhu mých studií lopatou házeli.

Prohlášení autora

Názory a závěry autora v této práci vyjadřují pouze jeho osobní názory a závěry a nepředstavují oficiální pozice jeho zaměstnavatele.

Anotace: Diplomová práce se zaměřuje na problematiku kybernetických konfliktů v postsovětském prostoru. Práce je svým pojetím rozdělena na dvě části. V první části se snaží o uchopení konceptu kybernetického konfliktu a představení teorie, která se k této oblasti váže. Jednotlivé koncepty kybernetického konfliktu nejsou v současné době ustáleny, práce se tak snaží o jejich utříbení a argumentuje použitelnost a dopady jednotlivých definic. Druhá část práce je věnována kybernetickým útokům na Estonsko v roce 2007, Litvu 2008, Gruzii 2008 a Kyrgyzstán 2009. V rámci těchto událostí se práce zaměřuje na průběh jednotlivých útoků, s důrazem na jejich širší kontext. Na základě popisu incidentů debatuje nad možnými příčinami konfliktů a vůbec konfliktní oblastí mezi pravděpodobnými aktéry.

Klíčová slova: kybernetické útoky, kybernetická bezpečnost, kybernetická válka, postsovětský prostor, výzkum konfliktů, Estonsko, Litva, Gruzie, Kyrgyzstán, Rusko

Annotation: The diploma thesis focuses on the issue of cyber conflicts in the post-Soviet space. Work is conceptually divided into two parts. The first part attempts to grasp the concept of cyber conflict and to present the theory that binds to this issue. The concept of cyber conflict is not currently steady, hence the work attempts to put together current theory and to discuss the applicability and impact of the various definitions. The second part is devoted to cyber-attacks against Estonia in 2007, Lithuania in 2008, Georgia in 2008 and Kyrgyzstan in 2009. In the frame of these events, the work focuses on the course of particular attacks, with an emphasis on their wider context. Based on the description of incidents, the thesis discusses the possible causes of conflict and conflict areas between probable actors.

Keywords: cyber-attack, cyber-security, cyber-war, post-soviet space, conflict research, Estonia, Lithuania, Georgia, Kyrgyzstan, Russia

Obsah

Počet znaků: 160 801

Úvod

Bylo napsáno mnoho textů, které se zabývají důsledky rozvoje informačních a komunikačních technologií pro celou společnost, a to včetně dopadů na jednotlivé společenské skupiny, ekonomiku státu, politiku státu, mezinárodní vztahy, právní řád apod.[1] Logicky má rozvoj informačních a komunikačních technologií také svůj významný dopad v oblasti bezpečnostní. Tyto technologie vedle schopnosti lépe komunikovat, vytvářet ekonomické či jiné hodnoty přinesly i možnost svou aktivitou de facto v reálném čase ovlivňovat dění v různých částech světa a zasahovat do bezpečnostní sféry mnoha subjektů.

Pokud byly dříve využívány počítače pouze jednotlivě pro provádění předem definovaných výpočtů, v současné době se využívají k nepřeberné škále činností. Jednotlivě stavěné stanice se postupně propojily do sítí pro zefektivnění všech navazujících procesů a lepší komunikaci mezi dalšími subjekty. Dříve nutné mezikroky, které prováděl člověk, byly z velké části automatizovány. Bankovní příkazy nepotřebují papírové formuláře, místo toho využívají elektronické prostředky komunikace a to jak ve vztahu banka-klient, tak i mezi bankami vzájemně. Státní správa komunikuje v čím dál větší míře elektronicky také jak mezi svými institucemi, tak s obyvateli státu. Armádní složky jsou závislé na správném fungování svých sítí a na souvisejících moderních technologiích. Zařízení veřejných služeb včetně elektráren či čističek odpadních vod jsou ve značné míře řízeny elektronicky, přičemž v množství případů je využito i dálkového řízení, tzn. že řídicí systém zařízení není oddělen od vnějšího světa, nýbrž je propojen do veřejných sítí elektronických komunikací (z drtivé většiny internetu). To pomáhá efektivitě řízení na jedné straně, nicméně to také vytváří další rizika.

Vzrůstající závislost jednotlivců, podniků a celých států na informačních a komunikačních technologiích je také zranitelností, které je možné využít. Pokud jsou propojeny systémy důležité pro chod státu, ekonomiku či jednoduše komunikaci mezi významnými subjekty, je na jejich správném fungování závislá bezpečnost státu a jeho obyvatel. Pokud jsou zároveň tyto systémy připojeny do veřejných sítí elektronických

[1] Nicméně jak uvádí Drmola (2014), ač bylo takových textů napsáno mnoho, stále existuje mnoho nejasností, jak kyberprostor a kybernetika obecně ovlivňují jednotlivé součásti společnosti.

komunikací, má jej na dosah teoreticky každý jiný připojený subjekt. To přináší prostor pro útočníky citelně zasáhnout důležité zájmy cílového subjektu. Využívání kybernetického prostředí pro dosahování politických cílů je pak jen logickým krokem.

Vezmeme-li v úvahu výčet významnějších konfliktů ve světě za poslední roky,[2] najdeme nemalý počet těch, které byly určitým způsobem vedeny i v kybernetickém prostředí.[3] Státy, zejména ty nejsilnější či nejvyspělejší, se postupně naučily využívat kybernetické prostředí i pro prosazování svých cílů. Zatímco cíleně destruktivní operace se v současné době téměř neobjevují[4], operace mířené na přerušení komunikačních schopností protivníka, omezení jeho fungování, či naopak krádeže strategických dat jsou využívány relativně často.[5]

Nejsou to však pouze státy, které se kybernetického boje v současné době účastní. Specifickým bezpečnostním aspektem kybernetického prostředí je totiž otevřenost či jeho přístupnost. Základ fungování nejrozšířenější sítě – internetu – dává každé stanici, každému jednotlivci značné možnosti ovlivnit de facto každý systém, který je k němu připojený. Kybernetické prostředí je tak charakteristické tím, že dává nestátním aktérům nemalý potenciál jak dosahovat významných až strategických cílů v rámci mezinárodní bezpečnosti (Rattray a Healey 2011).

Značné množství ukázkových případů kybernetických útoků v rámci konfliktů mezi jednotlivými státy se v relativně nedávné době událo v postsovětském prostoru. Jedná se například o často zmiňovaný kybernetický útok na Estonsko v roce 2007, díky němuž došlo ke značnému omezení služeb a fungování státní správy Estonska. V roce 2008 se

---

[2] Využívání kybernetického prostoru v rámci vedení konfliktů není tak novodobou záležitostí, jak bývá někdy prezentováno; děje se tak de facto od doby, kdy začaly být informační a komunikační systémy implementovány a používány pro činnosti, jejichž narušení může způsobit nějakou reálnou škodu či negativní reálný zásah. Tak například již v roce 1986 východoněmečtí hackeři sbírali informace z tisíců počítačů Spojených států, které následně prodávali KGB (Healey 2013: 10), stejně tak v roce 1999 při intervenci NATO v Kosovu, kdy Spojené státy omylem bombardovaly čínskou ambasádu v Bělehradě, nastal kybernetický útok zaměřený na vládní spojenecké sítě. Více k tomuto viz Healey (2013).

[3] Ať již to byl v omezené míře vpád Izraele do Libanonu v roce 2006, kdy došlo i na zásahy do informačních systémů, resp. webových portálů Hizbaláhu i Izraele (Saad a Bazan a Varin 2011). Stejně tak válka v Iráku, kdy bylo americkou armádou využito kybernetických útoků k rušení komunikace mezi Talibanem a Iráckými povstalci (Elliot a Payton 2010). Dále lze jistě zmínit konflikt mezi Ruskem a Gruzií v roce 2008 nebo poslední konflikt mezi Ruskem a Ukrajinou, kde taktéž bylo kybernetického způsobu boje využito.

[4] Popřípadě nejsou v současné době viditelné a rozeznatelné.

[5] Stejně tak je možné nalézt i značné množství kybernetických útoků odehrávající se mimo určitý konflikt, nicméně se značným dopadem do bezpečnostní sféry zasažených subjektů, jako například krádeže osobních údajů či know-how v rámci soukromé špionáže aj.

naopak odehrál ozbrojený konflikt mezi Ruskem a Gruzií, kde kybernetická kampaň ve značné míře ovlivnila konflikt omezením služeb státní správy Gruzie, sníženou konektivitou s ostatními státy kvůli zahlcení komunikačních sítí a zejména také sníženou schopností správně komunikovat a informovat o probíhajícím dění. Ve stejném roce se také odehrál kybernetický útok na Litvu v reakci na přijetí zákona o zákazu používání sovětských insignií na veřejnosti, pravděpodobně vedený z území Ruské federace (Tikk a Kaska a Vihul 2010). Zajímavým případem byl i kybernetický útok na Kyrgyzstán v roce 2009[6].

Tyto incidenty, které jsou vlajkovými případy rozsáhlého narušení kybernetické bezpečnosti států v postsovětském prostoru, se vždy odehrály v určitém kontextu vztahů mezi Ruskou Federací a zasaženým státem a měly svůj dopad i na širší mezinárodně-bezpečnostní situaci. Vzhledem ke kontextu incidentů zde vždy existovalo podezření na zapojení Ruské federace do těchto útoků, ať již přímo či nepřímo (srov. Thomas 2009: 476). Nikdy však nedošlo k jejich přičtení Rusku ať už z hlediska mezinárodně-právní či politické odpovědnosti a za aktéry těchto útoků byli označení nestátní aktéři, popřípadě zůstali neznámí.[7] Zkoumat přímé zapojení Ruské federace do těchto útoků je úkol obtížný, resp. v mnoha ohledech i takřka nemožný. Velmi dobrá popíratelnost aktivit a obtížné dokazování jsou totiž jedny z klíčových vlastností kybernetického prostředí (Applegate 2009, Carr 2009a). To však nemůže vést k rezignaci na zkoumání takových konfliktů.

Tato diplomová práce má za cíl na jednom místě popsat a analyzovat výše zmíněné incidenty (resp. kybernetické konflikty) při zvláštním zaměření na jejich kontext. Kontext je totiž prvkem, díky kterému je možné alespoň částečně omezit okruh možných aktérů a motivací útoků. Práce si neklade za cíl zjistit, jaké subjekty byly konkrétně za které útoky právně či politicky odpovědné. Záměrem je spíše analyzovat útoky společně s jejich okolnostmi, za kterých se odehrály. Nelze-li totiž určit přímou odpovědnost za rozsáhlé zásahy do běžného fungování napadených států, pak je

[6] Součástí práce není analýza kybernetických útoků na Ukrajině, zejména proto, že se jedná o stále probíhající, neukončený konflikt a nebylo by jej možné analyzovat podobně, jako výše uvedené konflikty. Vzhledem ke své podstatnosti je však i případ Ukrajiny zmíněn a diskutován v závěru práce.

[7] Debata nad uvedenými útoky je nicméně velmi obsáhlá. Často se však věnuje jednotlivým incidentům izolovaně, popřípadě se přesouvá pouze k jednotlivým aspektům, jako např. mezinárodně-právním dopadům těchto útoků, užitým technikám, kybernetickým strategiím států apod.

přinejmenším vhodné se zaměřit na průběh a okolnosti útoků a případně místo kauzality hledat alespoň korelaci s artikulovanými konfliktními událostmi.[8] Z povahy věci bude tato část práce pojímána primárně jako deskriptivně-analytická.

Vzhledem k současnému stavu teorie a uchopení této problematiky je záměrem této práce také diskutovat a vymezit význam kybernetického konfliktu a jeho navazujících pojmů s ohledem na obecný pojem konfliktu tak, jak je chápán v bezpečnostních studiích. V současné diskuzi se hovoří mnoho o kybernetické válce či konfliktech, z velké části však nejsou tyto pojmy zcela ustáleny. V souvislosti s kybernetickým konfliktem a válkou však vyvstává i množství navazujících fenoménů, které jsou s touto problematikou pevně spojeny – příkladem může být kybernetický terorismus, kybernetické povstalectví, hacktivismus, kybernetická kriminalita, aktivity tzv. klasických hackerů[9] apod. Není záměrem práce tyto fenomény nově konceptualizovat, ale spíše je správně vymezit a pokusit se je napojit na koncept kybernetického konfliktu.

V rámci celé práce pak budou řešeny následující výzkumné otázky:

1. Jakým způsobem je v současné době chápán pojem kybernetického konfliktu? Jak zapadá či doplňuje obecné chápání konfliktu v bezpečnostních studiích? Jaké jsou na tento koncept hlavní navazující pojmy a jakým způsobem se váží ke kybernetickému konfliktu?
2. Jakým způsobem a za jakých okolností proběhly kybernetické útoky na Estonsko v roce 2007, na Gruzii a Litvu v roce 2008 a Kyrgyzstán v roce 2009?

Výstup práce může jednak pomoci lépe pochopit koncepty v oblasti kybernetické bezpečnosti a konfliktů, a dále také přispěje k osvětlení kybernetických konfliktů v post-sovětském prostoru.

[8] Nález podobné korelace u vícero případů pak je jistě pro další výzkum lepším východiskem než-li pouze u případu jediného.

[9] Význam pojmu „klasický hacker“ je v této souvislosti použít ve shodě s definicí Roba Sheina (2010), který takto označuje osoby s výjimečnými znalostmi a talentem, nicméně s benevolentními motivacemi. Jejich klíčovou motivací nebyl prospěch či poškození druhé strany, naopak to byla snaha o zisk vědomostí, dalších zkušeností a snad i úspěchů, které jiným způsobem nebyli možní získat.

1. Metodologie práce

Položené výzkumné otázky vyžadují, aby se práce zaměřila na určité aspekty sledovaných kybernetických útoků postupně. Proto je tato práce postavena na několika částech.

Nejprve se práce zaměří na teorii kybernetického konfliktu. Důvodem je nutnost určitého teoretického ukotvení dané problematiky, a vůbec vymezení oblasti zkoumání vzhledem k existující rozpolcenosti v užívání některých souvisejících pojmů. Cílem této části je přispět k následnému jasnějšímu vymezení konceptů vážících se k daným incidentům a jejich částem, které si práce klade za cíl popsat a analyzovat. Základním problémem bude vymezení pojmu kybernetického konfliktu, války a útoku; pokud se například podíváme na kybernetické útoky, lze jich v současné době nalézt celou řadu, nicméně mají různé charakteristiky, jsou prováděny různými způsoby v různých kontextech, různými aktéry a zejména s různými cíli.

I přesto, že je teorie kybernetické bezpečnosti a kybernetického válčení v současné době relativně dobře zpracována, trpí částečně definičními a hlavně konceptualizačními rozpory.[10] I proto je správné vymezení zkoumaného fenoménu zásadní. Práce bude vycházet ze současné odborné literatury, odborných textů a komentářů ke zkoumaným fenoménům. Nedrží se teorie jednoho autora – naopak díky syntéze a porovnání chápání jednotlivých konceptů mohou být dané pojmy lépe vytyčeny a popsány.

Následně se práce zaměří na analýzy jednotlivých kybernetických útoků. Útoky na Estonsko, Litvu a Gruzii jsou již v současné odborné literatuře relativně dobře zpracovány, práce proto bude vycházet zejména ze sekundárních zdrojů, které jsou k těmto incidentům k dispozici. K dispozici není mnoho analýz kybernetických útoků na Kyrgyzstán v roce 2009. Hlavními zdroji k tomuto incidentu budou zejména články z novinových a odborných periodik, stejně jako budou využívány komentáře, které se k němu mezi odbornou veřejností objevily.

[10] Příkladem může být pojem kybernetického útoku, pod nějž například jistá část odborníků na mezinárodní právo zahrnuje i klasické konvenční útoky na informační a komunikační infrastrukturu (viz např. Hathaway 2012); s tímto by značná část teoretiků kybernetického válčení nesouhlasila (Healey 2013). Valeriano a Maness (2014) naopak pojem kybernetického útoku odmítají právě z důvodu jeho zavádějícího charakteru. Viz dále v této práci.

Nejprve je vždy představen kontext, ve kterém se jednotlivé útoky odehrály, následně jsou popsány incidenty samotné se zaměřením na cíle, způsoby a případné aktéry provedených útoků. Součástí analýzy jsou i dopady a události, které se odehrály bezprostředně po útocích. Poslední části je pak analýza vztahu útoků a existujících konfliktů mezi možnými aktéry. Výběr těchto definovaných oblastí je dále v této práci konkretizován.

Po částech věnujících se teoretickému uchopení kybernetického konfliktu a analýze jednotlivých incidentů se práce zaměří na diskuzi k výskytu a dopadům představených útoků a jejich okolnostem.

2. Kyberprostor a kybernetické konflikty – vymezení pojmů

Kybernetika je pojmem, který zejména v posledních letech nabývá na významu v mnoha oblastech života a společnosti. Snad její zrod za pomoci výzkumu a vývoje v oblasti informačních a komunikačních technologií znamenal, že se velmi dlouho tato problematika přenechávala zejména technickým oborům, a méně se upírala pozornost na dopady společenské. V současné době, kdy je společnost svědkem čím dál častějšího a rozšířenějšího zneužívání této domény, již tomu tak není a naopak lze zaznamenat značný rozvoj i společensko-vědního uchopení této problematiky. Nejen akademická sféra a veřejnost si nyní uvědomuje její dopad na každodenní život a chod společnost, i samotné státy se rozhodly daleko více zaměřovat na kybernetiku a zejména kybernetickou bezpečnost a obranu, v rámci kterých se snaží rozvíjet své kapacity.

Jak již bylo v předchozích částech práce řečeno, je řádné vymezení současné teorie kybernetického konfliktu pro správný popis a zasazení zkoumaných incidentů do širšího rámce esenciální.

V této kapitole se práce zaměří na vymezení společensko-vědních pojmů a konceptů vlastních kybernetické bezpečnosti. Nejprve představí pojem kybernetického prostoru (nebo také kyberprostoru) jako ústředního konceptu popisující toto prostředí sui generis. Poté se přesune k dalším souvisejícím pojmům, jako je kybernetický útok, kybernetický konflikt, kybernetická válka aj. V samostatné podkapitole budou v krátkosti rozebrány koncepty kybernetické kriminality, hacktivismu, kyberterorismus, kyberpovstalectví, klasického hackingu a patriotického hackingu.

2.1. Kybernetický prostor

Jak bylo naznačeno v úvodu, celá společnost se postupně stává na správném fungování informačních a komunikačních systémů závislá; tyto technologie vstupují do mnoha různých částí životů lidí a společností a často nahrazují lidskou činnost kritické povahy. Kybernetický prostor vznikl na základě fungování těchto technologií, nicméně se jedná o pojem, jenž vymezuje vlastní předmět, který neoznačuje pouze existenci těchto technologií samotných.

Je známo, že poprvé byl tento pojem použit Williamem Gibsonem v díle Neuromancer, kde jej popsal jako *„konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům ... grafické*

zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat" (Macek 2003). Tento popis je často diskutován zejména vzhledem k jeho neuchopitelnosti (Rid 2013: 164), nicméně se na něj, možná právě kvůli své abstraktnosti, spousta definic stále odvolává. Je zajímavé, do jaké míry se tento pojem vyvíjel zejména s ohledem na rozvoj technologií a propojování systémů do velké sítě prostřednictvím internetu. John Perry Barlow (1996) a poté i David Hakken (1999) se vyjádřili ke konceptu kyberprostoru v tomto duchu, nicméně i oni sami však nakonec odkazují ke kyberprostoru jako k určitému druhu kultury. I přes zakomponování technického prostoru stále pro ně zůstává pojmem spíše sociální či kulturní antropologie (Macek 2003, Morrison 2009).

V současné době není nazírání na pojem kybernetického prostoru jednotné. Dle Kramera (2009: 4) existuje 28 různých definic kyberprostoru.[11] Sám pak souhlasí s definicí Kuehla (2009: 26) kyberprostoru jako *„globální domény v rámci informačního prostředí, jehož odlišující a unikátní charakter je ohraničen použitím elektroniky a elektromagnetického spektra k vytvoření, uchovávání, modifikování, výměny a využití informací skrze závislé a propojené sítě využívající informační a komunikační technologie"*.[12] K tomuto Kramer (2009) uvádí, že se jedná o široké vymezení, které zdůrazňuje spíše technickou povahu tohoto prostoru, než povahu kulturní.

Technickou povahu kyberprostoru podtrhuje ve své definici i Healey (2013: 280). Ten jej popisuje jako *„propojené informační technologie"*[13]. Dle něj existují mnohem komplexnější definice, nicméně základním kamenem kyberprostoru jsou jakékoli systémy, které uchovávají či zpracovávají informace a jsou propojeny do určité sítě. Takový celek pak lze označit za součást kyberprostoru. Konkrétnější definice jsou pak neefektivní, jelikož se stanou zastaralými hned poté, co jsou sepsány; platnost výše uvedeného popisu má tendenci vydržet déle (Tamtéž).[14] Podobný náhled je možné vidět i u dalších autorů např. Rattray (2001) nebo Denning (1999).

[11] Je nicméně nutné říci, že k tomuto číslu došel pouze jeden výzkum (Kramer 2009), skutečný počet definicí může být opravdu odlišný již z toho důvodu, kolik různých subjektů jej pro své zájmy definuje.
[12] Překlad autora této práce.
[13] Překlad autora této práce.
[14] Překlad autora této práce.

Nazírání na kybernetický prostor ve smyslu technického fungování a zabezpečení jako prostředí svého druhu je společným jmenovatelem i většiny současných národních strategií kybernetické bezpečnosti či jiných politik jednotlivých zemí.[15]

Za zmínku zde stojí definice Oxfordského slovníku jako *„teoretické prostředí, ve kterém se odehrává komunikace skrze počítačovou síť“*[16] nebo definice použita v Kanadské strategii kybernetické bezpečnosti (2010): *„Kyberprostor je elektronický svět vytvořený propojenými sítěmi informačních technologií a informacemi těchto sítí. Jedná se o celosvětový společný statek,*[17] *ve kterých je více než 1,7 miliardy lidí propojeno, aby sdíleli myšlenky, služby a přátelství.“*[18]

Lze tak vidět, že ač jsou definice daleko lépe zasazeny do současného technologického fungování globálních sítí, některé z nich stále předpokládají různé aktivity jednotlivců (srov. Zimet a Skoudis 2009) od výměny dat až po mezilidskou komunikaci (a dle Kanady také k navazování přátelství). Tento prvek je naprosto zásadní a do jisté míry vrací kyberprostor zpět do dřívějšího rámce poukazujícího na existenci a interakce lidské společnosti.

Není cílem práce zaobírat se různými definicemi kyberprostoru, spíše je zde snaha o dokázání nejednotnosti chápání tohoto pojmu, který je odrazovým můstkem pro další vymezení. Je kyberprostor celosvětový společný statek zahrnující množství lidských interakcí nebo je pro něj určující pouze existence pevné infrastruktury na území jednotlivých států? Platí-li prvé, do jaké míry na něj dopadají jurisdikce jednotlivých států, které tak mohou, resp. mají zasahovat do jeho obsahu? Do jaké míry pak vůbec

---

[15] Například českou definici je možné nalézt v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, kde se v § 2 písm. a) uvádí, že *„kybernetickým prostorem* (pozn. - se rozumí) *digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* Německá definice obsažená ve Strategii kybernetické bezpečnosti pro Německo (2011) konkrétněji rozvádí i jednotlivé prvky a fungování kyberprostoru: *„Virtuální prostor všech IT systémů spojených na datové úrovni v globálním měřítku. Základem kyberprostoru je internet jako univerzální a veřejně dostupné spojení a spojovací síť, která může být doplňována a dále rozšiřována počtem přídavných datových sítí. IT systémy v izolovaném virtuálním prostoru nejsou součástí kyberprostoru.“* Další definice viz např. webový portál NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/cyber-definitions.html.

[16] Překlad autora této práce.

[17] V originálním znění je použit výraz „global commons“, který se do češtiny obecně překládá jako „společné dědictví lidstva“ a který odkazuje na společné, nikým nevlastněné prostory země, které jsou určeny k využití celému lidstvu. V tomto případě je použit termín „celosvětový společný statek“ zejména z toho důvodu, že kyberprostor není něco zděděného, co by existovalo i bez přítomnosti lidstva.

[18] Překlad autora této práce.

mohou státy ovlivňovat jednání jednotlivých uživatelů v rámci celosvětové sítě? Nejen tyto otázky se odvíjí od vymezení kyberprostoru; nejedná se tak pouze o samoúčelnou akademickou debatu.

Důvodem, proč je relativně obtížné přesně kyberprostor vymezit je i skutečnost, že se neustále rozšiřuje a zasahuje do dalších sfér společnosti, přičemž od existence prvních sítí tvořených několika počítači se změnil k nepoznání (Singer a Friedman 2014).

Pro potřeby této práce je možné na kyberprostor nejlépe nahlížet jako na prostředí tvořené informačními a komunikačními technologiemi, které umožňují výměnu dat a komunikaci mezi dvěma nezávislými systémy zejména (nikoli však pouze) prostřednictvím nejrozšířenější sítě, tj. internetu. Kyberprostor je také prostorem, který je využíván jednotlivými subjekty k nepřeberné škále činností zahrnující tvorbu, zpracování a výměnu dat. Takto je obsažena jak virtuální a „společenská" stránka problematiky, tak také její fyzická část v podobě existence potřebné infrastruktury (srov. Libicki 2007). I díky ní je možné souhlasit s vymezením kyberprostoru dle Singera a Friedmana (2014), které odmítá kyberprostor jako celosvětový společný statek: *„Kyberprostor může být globální, ale není ‚bezstátní' nebo ‚celosvětový společný statek', oba termíny hodně užívané vládami a médii. Stejně jako jsme my, lidé, uměle rozdělili zeměkouli na teritoria, které nazýváme ‚národy', a zároveň lidský druh na různé skupiny nazvané ‚národnosti', to stejné může být učiněno s kyberprostorem. Ten je totiž závislý na fyzické infrastruktuře a lidských uživatelích, kteří jsou spojeni s určitým teritoriem, a proto jsou předmětem našich lidských pojmů jako suverenity, národnosti, vlastnictví"*[19] (Singer a Friedman 2014: 14). Hned vzápětí však dodávají, že i když není kyberprostor ‚bezstátní' nebo nezávislý na teritoriu, tak je jeho geografie o mnoho více nestálá než v jiných prostředích. Přesunout horu nebo část vodstva vždy trvá delší dobu, v kyberprostoru je možné překonat vzdálenosti během milisekund (Tamtéž).

Ač se tedy vzdálenosti při komunikaci stírají, není kybernetický prostor nezávislý na skutečné geografii světa a teritoriu umístění informační a komunikační infrastruktury.[20]

[19] Překlad autora této práce.

[20] V kontextu kybernetických útoků může být zvláštním důkazem závislosti kyberprostoru na geografických podmínkách tzv. pulzní DoS útok, který využívá rozsáhlosti infrastruktury a většinou také geografických vzdáleností pro koordinovaný zásah cíle takovým způsobem, že v průběhu určité doby je vysíláno zdrojovým systémem mnoho požadavků různými, předem

Některé státy běžně ovlivňují přenos informací mezi svým územím a územím jiných států, ať již přímo skrze blokování komunikace s určitými servery[21], popřípadě odvozeně ve formě trestního postihu při porušení daných pravidel[22]. Státy nemusí mít svůj kyberprostor zcela pod svou kontrolou (ať již z důvodů politických či technických), nicméně tvrzení, že se jedná o svobodný prostor bez pravidel, je zavádějící. I přesto, že kyberprostor poskytuje mnoho příležitostí a možností jednat pro velmi široký okruh subjektů, státy na tato jednání v něm vždy budou mít vliv, podobně jako mají vliv i na další prostředí a oblasti společnosti.

2.2. Kybernetická bezpečnost

Kybernetická bezpečnost se od vymezení kybernetického prostoru odvíjí, přičemž i zde existuje mnoho různých definic. Healey (2013: 281) ji definuje jako veškeré aktivity k ochraně počítačů a sítí od útoků na jejich důvěrnost, integritu a dostupnost. Dívá se však na ni zejména jako na technický pojem, kdy člověk s expertízou v kybernetické bezpečnosti nemusí být expertem na kybernetický konflikt a naopak.

S odmítnutím stejného předmětu kybernetické bezpečností a konfliktu lze souhlasit, méně však lze souhlasit s pojetím tohoto pojmu spíše technicky. Pokud přijímáme kyberprostor jako něco skládajícího se z informačních a komunikačních technologií, virtuálních dat a případně i z lidských interakcí, pak je nutné kybernetickou bezpečnost pojmout jako kombinovanou bezpečnost všech těchto prvků. Nelze totiž uvažovat, že kybernetická bezpečnost je zajištěna, pokud jsou zabezpečeny veškeré technické prvky systémů a sítí. Základem kybernetické bezpečnosti totiž zůstává člověk a jeho působení v kyberprostoru – při mnohých (nikoli však všech) typech kybernetických útoků to bývá právě člověk a jeho jednání, které je nejslabším článkem a které nakonec způsobí nejvýraznější škodlivé efekty.

Například nová česká Národní strategie kybernetické bezpečnosti pro období let 2015 až 2020 ji definuje jako *„souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a*

---

určenými směry s předem vypočítanou odezvou tak, aby všechny požadavky zasáhly a zahltily cíl v jeden daný okamžik.

[21] Jedná se zejména o země neliberální. Jako typický příklad lze uvést Čínu.

[22] Tento případ se již odehrává i ve většině liberálních států – pokud je obsah přenášených informací v rozporu s právním řádem, pak je možné pachatele stíhat. Typicky se jedná např. o případy počítačového pirátství, dětské pornografie apod.

odolného kyberprostoru […] Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.“

Technická opatření jsou jen částí kybernetické bezpečnosti – ta zahrnuje velké množství dalších oblastí, od politických a právních, po vzdělávací. Kybernetika a kybernetická bezpečnost tak není pojmem technickým jako spíš pojmem společenským. A není to pouze záležitost příčin incidentů; pokud přestanou informační a komunikační technologie správně fungovat, dopad to bude mít opět zejména na lidi a společnost, jelikož ty jsou hlavními příjemci užitku jejich provozování (Luht 2014).

V obou představených definicích je pak kybernetická bezpečnosti představena oproti bezpečnosti v bezpečnostně-politické oblasti (viz Zeman et al. 2002) ne jako určitý stav, ale spíš jako prostředky, kterých má být dosaženo nerušené používání kyberprostoru.

Kybernetická bezpečnost tak pro jednotlivé státy zejména představuje schopnost nejen zajistit informační a komunikační systémy technicky, nýbrž celkově i skrze působení na jednotlivce a skupiny obyvatelstva, ať již právně, politicky, vzděláním či jiným způsobem.

2.3. Kybernetický útok

V dnešní společnosti se není možné vyhnout záplavě informací o kybernetických útocích, ať již v mezinárodním kontextu při konfliktu států, nebo v kontextu kriminálním při krádežích dat a poškozování jednotlivců či obchodních společností. Tento pojem nabývá různých významů v různých společensko-vědních a technicko-vědních oblastech.

Pro správné vymezení pro potřeby této práce je možné se odrazit od definice, kterou nabízí Loreents a Ottis (2010: 140) ze CCDCOE: *„Kybernetický útok je záměrné užití kybernetické zbraně nebo systému, který může být použit jako kybernetická zbraň, proti informačnímu systému s cílem způsobit kybernetický incident.“*[23] Kybernetickou zbraní je pak systém založený na informačních technologiích, který je přímo určen k poškození struktury nebo operací jiného informačního systému (Lorents a Ottis 2010: 139-140).

[23] Překlad autora této práce.

Tato veskrze technická definice je platná, nicméně nezahrnuje i další existující chápání (a běžná užívání) tohoto pojmu.

Sám Healey (2013: 280) tvrdí, že za kybernetický útok je zpravidla označován čin, při kterém je obecně užito počítače nebo sítě k zlomyslnému ovlivnění jiných počítačů a sítí, nicméně dodává, že je tento pojem rozličně vnímán odborníky z různých oborů; vojenští představitelé hovoří o potenciálním válečném aktu, instituce zabývající se vymáháním práva hovoří o útoku jako trestném činu, techničtí specialisté jej pak vidí jako zejména zneužití společného prostředku.

Příkladem může být např. Hathaway (2012), která ač navazuje na širší diskuzi oblasti kybernetického konfliktu, se na pojem kybernetického útoku dívá spíše z právní perspektivy – vychází přitom z vládních koncepcí chápání tohoto pojmu jako záležitosti národní bezpečnosti, když komentuje přístup Spojených států ve srovnání s Organizací Šanghajské spolupráce. Ve své práci k právu kybernetických útoků nakonec dochází k následující definici: *„Kybernetický útok je jakýkoli čin sloužící k podkopání fungování počítačového systému pro politický nebo národně-bezpečnostní záměr“*[24] (Hathaway et al. 2012: 10). Svým přístupem se tak oprošťuje od technického pojetí útoku, kdy se jedná o aktivitu používající počítač nebo síť; naopak zdůrazňuje, že se jedná o jakýkoli čin, který je namířen proti počítačovým sítím s politickým cílem, přičemž škodlivá aktivita může být i kinetická a nemusí se jednat pouze o využití systémových zranitelností vůči konkrétnímu cíli.

Tento přístup je však velmi rozporuplný. Umožňuje totiž za kybernetický útok považovat i bombardování komunikační infrastruktury, nikoli však již ovládnutí dronu hackerem a jeho útok na pozice v jiné části světa. Při definici kybernetického útoku se totiž Hathaway zaměřuje na cíl, kterým je kyberprostor samotný – pokud aktivita nepoškozuje kyberprostor, pak se o kybernetický útok nejedná. Je snad ovlivněna právním zaměřením autorky, kde kybernetický útok v technickém slova smyslu nemusí být útokem ve smyslu právním, který je vlastní zejména humanitárnímu právu; jistě je však ovlivněna pohledem na kyberprostor jako na pouhou další doménu vojenství. Stejně jako je cílem pozemních sil udržet pod kontrolou území státu (bez ohledu na použité způsoby), stejně tak jsou kybernetické síly zaměřeny na udržení funkčnosti kyberprostoru (Tamtéž). Autor této práce se domnívá, že tato definice se příliš vzdaluje

[24] Překlad autora této práce.

od obecného chápání kybernetického útoku nejen v odborné, ale i laické sféře. Zároveň zaměňuje oborově zaměřené a obecné chápání tohoto pojmu[25]; pokud totiž hovoříme o pozemní doméně, má předložená analogie smysl. Pokud však hovoříme o pozemním útoku, hovoříme o způsobu, nikoli cíli.

Jen pro úplnost nejasnosti pojmu ‚kybernetického útoku' v současných společensko-vědních debatách je možné dodat definici Dipperta (2013) společně s jeho vysvětlením. Ten jej rozděluje na pojem v širším a užším slova smyslu. V širším smyslu se jedná o akt kybernetické špionáže, hacking nebo pokus o něj k získání strategických či komerčních dat; může to být také blokování stránek nebo použití defacementu[26] atd. V užším slova smyslu používá termín „cyberwarfare attack", který pak definuje jako způsobení úmyslné újmy jedním státem informačnímu systému druhého státu pomocí kybernetických prostředků. Ač v oblasti vojenství zůstává při definici v rámci užitých prostředků a způsobů, oproti Hathaway (2012) (možná zbytečně) přidává pouze státy jako vykonavatele a oběti útoků. Tímto však vylučuje problematiku nestátních aktérů, která (jak bylo již v úvodu naznačeno) je pro oblast kybernetické bezpečnosti a kyberprostoru nadmíru důležitá.

Jak se tedy na pojem kybernetického útoku dívat? Podobně jako při definici kyberprostoru, i zde je obtížné dát odpověď ideálně pro co nejširší míru společensko-vědních oborů. Tato práce se kloní k techničtější definici pojmu, kdy kybernetickým útokem je myšlena jakákoli úmyslná škodlivá aktivita vykonávána prostřednictvím informačních a komunikačních systémů zaměřena na narušení důvěrnosti, integrity nebo dostupnosti dat, bez ohledu na skutečnost, zdali způsobí skutečnou vyčíslitelnou škodu či nikoli, resp. bez ohledu na její právní či jiný dopad a bez ohledu na to, zdali je cílem či původcem stát nebo jiný aktér. Důvodů pro toto vymezení je několik; snažili-li bychom se vymezit kybernetický útok perspektivou oboru svého zkoumání, pak bychom se velmi pravděpodobně dostali do rozporu s jinými obory. Má-li být teorie kybernetického konfliktu jako společensko-vědního fenoménu ucelená, musí existovat

[25] Podobně jako je „útok" konceptualizován odlišně v obecném mezinárodním právu veřejném a mezinárodním právu válečném.

[26] Jedná se o speciální typ kybernetického útoku. Slovník ke kybernetické bezpečnosti jej definuje následovně: *„Průnik do webového serveru protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. Zkreslení není skrytí, naopak, usiluje o medializaci a jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka"* (Jirásek a Novák a Požár 2013).

co možná nejuniverzálnější definice kybernetického útoku. Technické vymezení neřeší motivace, charakter či cíle útočníků nebo právní problematiku jejich dopadů – tyto pak mohou být řešeny až v navazujících krocích. Pod kybernetický útok tak mohou spadat špionážní aktivity, čistě kriminální aktivity spočívající v překonávání bezpečnostních opatření systémů a krádeži dat, stejně jako rozsáhlé útoky podniknuté nestátním aktérem či státem způsobující dlouhodobou nedostupnost systému.

Pro úplnost je vhodné vymezit i pojem ‚kybernetický incident', který je v této práci taktéž používán. Ač i zde existuje vícero definicí, je vhodné jej pro potřeby této práce vymezit jako událost, která způsobuje nebo může způsobit nepřijatelné deviace ve struktuře či činnosti informačního systému či jeho součástí (Loreents a Ottis 2010). Podobně jej vymezuje např. i Komise pro Národní bezpečnostní systémy[27] vlády Spojených států (CNSS 2010). Na jedné straně tak jsou pod incidenty zahrnuty jak intencionální aktivity, tak i neintencionální. Každý kybernetický útok bude kybernetických incidentem, každý incident již však nemusí být útokem.

2.4. Kybernetický konflikt

Pojem ‚kybernetický konflikt' je v případě této práce zásadní. Pokud je cílem analyzovat v úvodu vymezené útoky se svými kontexty, aktéry, cíli a dopady, pak je nutné správně konceptualizovat i kybernetický konflikt. Oproti techničtěji definovaným pojmům kyberprostoru nebo kybernetického útoku je pojem konflikt pojmem zejména sociálně-vědním. Ve vymezení konceptu kybernetického útoku je proto vhodné se od něj odrazit. Konflikt sám je však mnohovrstevným fenoménem v mnoha společensko-vědních oblastech (Šmíd 2010). Existuje celá řada jeho pojetí a zejména přístupu k němu; vzhledem k tématu práce je lépe se zaměřit na jeho pojetí v rámci bezpečnostního výzkumu, konkrétně pak na konfliktologické pojetí se zaměřením na jeho příčiny, projevy, charakteristiku aktérů apod. Práce tudíž nebude primárně zaměřena na konflikt ve smyslu zkoumání válečnictví a vedení boje (tj. se záměrem řešit strategické, taktické a operační cíle jednotlivých aktérů při vzetí v potaz jejich silné a slabé stránky, stejně jako jejich příležitosti a hrozby). Problematice kybernetického válečnictví se práce věnuje jen částečně, zejména v bodech, ve kterých je úzce spojena s výzkumem konfliktu v obecném smyslu.

[27] Jedná se o meziresortní organizaci americké vlády, která je zodpovědná za bezpečnostní politiku bezpečnostních informačních a komunikačních systémů Spojených států.

Pšeja (2002: 52) jej definuje jako střet mezi jasně definovatelnými aktéry, kteří usilují o uplatnění svého zájmu v jedné nebo více shodných oblastech, přičemž tito aktéři pociťují vzájemný střet jako situaci, kdy zisk jedné strany znamená ztrátu druhé. Pro její analýzu pak využívá charakteristik, které konfliktu přisuzuje Holsti (1983) (dle Pšeja 2002, Šmíd 2010):

1) musí mít **aktéry**, jimiž jsou standardně státy, třebaže narůstá frekvence případů, kdy se na konfliktech podílejí i aktéři nestátní;
2) musí mít jasně definovatelnou **oblast střetu**, která je náplní konfliktu;
3) musí být přítomno **napětí**[28], které funguje jako predispozice konfliktu a které je typicky vyjádřeno v postojích, jako je nedůvěra apod.;
4) nutnou složkou konfliktu je pak **jednání**, které má podobu opatření a kroků realizovaných stranami konfliktu.

Dle Šmída (2010) je možné uvažovat o konfliktu i za předpokladu, kdy chybí čtvrtý, či ve výjimečných případech i třetí bod výše zmíněných charakteristik. Zároveň pak udává nejdůležitější rozdělení konfliktů, ať už z hlediska zapojení stran, přítomného jednání nebo oblasti střetu. Z hlediska příčin lze uvést rozdělení na konflikt zájmů a konflikt hodnot. Z hlediska zájmů pak na konflikty o území, ekonomické či politické. Z hlediska hodnot pak lze hovořit o konfliktech etnických, náboženských, ideologických apod.

Ani zde není cílem opakovat teorii a debatu nad vymezením konfliktu samotného v bezpečnostních studiích. Cílem je spíše poukázat na problematiku zařazení ‚kybernetického konfliktu' do ‚konfliktu' obecně (bezpečnostně-vědně) chápaného. Proto, než práce přistoupí k této diskuzi, je vhodné představit současné definice ‚kybernetického konfliktu' samotného.

Healey (2013) uvádí, že se jedná o určitý stav, kdy národy a nestátní aktéři užívají útočné a obranné kybernetické kapacity k útoku, obraně nebo špehování druhého státu, typicky kvůli politickým nebo jiným národně-bezpečnostním důvodům. Obecně

[28] Bartos a Wehr (2002) používají přímo výraz ‚nepřátelství' (hostility). Při hlubším srovnání s Holsti (1983: 400) nelze vyvozovat zásadní odlišnosti ve vymezení významů těchto pojmů, ač sémanticky je nepřátelství důrazněji namířené proti druhé straně. Právě díky směřování negativních postojů explicitně vůči druhé straně konfliktu je v této práci použita terminologie dle Holsti, jelikož ta je daleko citlivější k oblasti (předmětu) konfliktu bez předjímání nenávisti jako příčiny konfliktu (grievance dle Bannon a Collier [2003]).

kybernetický konflikt nezahrnuje kybernetickou kriminalitu, ale zato je nadřazeným pojmu ‚kybernetická válka'.[29]

Mulvenon a Rattray (2012) jej pak definují jako politicky motivované konfliktní jednání velkého rozsahu založené na užití útočných a obranných kapacit s cílem narušit digitální systémy, sítě a infrastrukturu, včetně použití kybernetických zbraní a nástrojů státními, nestátními či transnacionálními aktéry ve spojení s dalšími prostředky dosahování politických cílů. Alternativně jej pak vymezují také oproti pojmu kybernetické války, která je dle nich užším pojmem. Kybernetický konflikt obsahuje veškeré konflikty a nátlakové aktivity mezi národy nebo skupinami se strategickými cíli za využití kyberprostoru, kde software, počítače a sítě jsou použity jako prostředky i jako cíle jednotlivých útoků (Tamtéž).

Valeriano a Manes (2014) při definování kybernetického konfliktu sice vycházejí z definic vlastních kybernetickému válčení (warfare), přičemž nakonec dochází k závěru, že je jím rozuměno využití výpočetní techniky v kyberprostoru ke zlomyslným a škodlivým účelům s cílem ovlivnit, změnit nebo modifikovat diplomatické a vojenské interakce mezi entitami, které nejsou ve válce, mimo konvenční bojiště.

Nakonec Loreents a Ottis (2010: 140) považují za kybernetický konflikt použití kybernetických útoků, které musí zahrnovat útoky proti integritě nebo dostupnosti systému, k dosažení politických cílů.[30] Politické cíle jsou pak jakýmsi zastřešujícím atributem, který popisuje hlavní důvod útoku (Loreent a Ottis 2010: 140).

Lze vidět, že veškeré představené definice operují zejména s politickým cílem jako zastřešujícím atributem útočných a obranných aktivit v rámci kybernetického prostoru mezi jednotlivými aktéry hájícími právě opačné pozice. Naopak zde chybí požadavek existence napětí mezi danými aktéry – to však může být implicitní již konkrétnímu konfliktnímu jednání. Zároveň lze vypozorovat, že základními útoky při kybernetických konfliktech jsou útoky na dostupnost a integritu dat a systémů, důvěrnost přidává pouze

[29] Viz podkapitola 2.5. této práce.

[30] Požadavek na zásah do integrity nebo dostupnosti vychází z potřeby rozlišit kybernetický konflikt od kybernetické špionáže; vezmeme-li například špionáž, pak ta sice často bývá součástí kybernetického konfliktu, sama o sobě však nemusí způsobovat žádnou škodu, poškození. Přímo poškození systému (zásah do integrity) nebo jeho omezení použitelnosti (zásah do dostupnosti) způsobuje per se určitou škodu na systému či datech samotných.

Healey (2013). Důvěrnost je cílem zejména při špionážních kybernetických útocích, které ač prováděny s určitým politickým cílem, nemusí být nutně prováděny v rámci kybernetického konfliktu, jelikož zde může chybět definovatelná oblast střetu.[31, 32] Snaha získat další neveřejné informace nemusí a priori znamenat existenci konfliktu.

Je pak vhodné se ptát, jakým způsobem je možné nahlížet na kybernetický konflikt z pohledu obecné teorie konfliktu. Autor této práce má za to, že kybernetický konflikt je podřazen konfliktu obecnému, přičemž uvozuje spíše aktuální škodlivé aktivity mezi jednotlivými aktéry a nelze jej považovat za konflikt sui generis.[33, 34] Oproti obecné teorii konfliktu tak například nehovoříme o kybernetickém konfliktu ve fázi latence, popř. často ani ve fázi artikulace konfliktu, kdy jsou pouze vyjádřeny zájmy a hodnoty (resp. oblast), kde dochází ke střetu, přičemž samotné konfliktní jednání ještě není přítomno. O kybernetickém konfliktu v užším slova smyslu hovoříme až tehdy, dojde-li k používání informačních a komunikačních technologií s cílem narušit dostupnost nebo integritu dat či systémů protivníka k dosažení jinak neslučitelných politických cílů. V širším slova smyslu je pak možné za kybernetický konflikt označit takový konflikt, který se svým přítomným jednáním odehrává převážně v kyberprostoru.

2.5. Kybernetická válka

Pokud bychom hledali pojem, který je v rámci řešené problematiky nejdiskutovanější a jeho chápání je nejméně jednotné, mohli bychom velmi snadno dojít ke ‚kybernetické válce'. Základním problémem je jednak nadužívání tohoto pojmu, zčásti však také jeho nejasné vymezení - v rámci odborné komunity není tento pojem používán jednotně.

---

[31] Pro úplnost je nutné dodat, že trojice „dostupnost – integrit – důvěrnost" jsou navzájem velmi úzce propojeny a často narušení jednoho prvku může způsobit i narušení prvku druhého.

[32] Z hlediska zasazení kybernetického konfliktu do širšího rámce využívají někteří autoři (např. Schmitt 2015) pro vymezení i rozdělení na (i) pouze kybernetický konflikt, a (ii) kybernetický konflikt jako součást širšího ozbrojeného konfliktu.

[33] Je tedy pojmem daleko blíže výzkumu vedení války (válečnictví) než výzkumu konfliktu, jelikož hlavní předmět zkoumání – aktéři a jejich motivace – sám kyberprostor neurčuje. Politické cíle jsou zpravidla mimo kyberprostor samotný. Viz dále.

[34] Určitou analogii lze spatřit s pojmem hybridní válka – v současné době se o tomto konceptu hovoří jako o něčem novém, odlišném oproti původní „válce". Lze však spíše souhlasit s těmi, kteří považují hybridní válku za pouhou variaci války běžné, přičemž k dosažení politických cílů jsou používány jiné, pro současnou dobu efektivnější prostředky. Pojem „hybridní válka" pak označuje pouze subtyp konfliktního jednání mezi aktéry.

Podobným způsobem, jako bylo dříve (a někdy stále je) nutné vymezovat v rámci výzkumu konfliktu pojmy ‚válka' (war) a ‚válečnictví' (warfare)[35], čelí podobné výzvě i oblast kybernetické bezpečnosti.

V současné době lze také například narazit na tvrzení, že kybernetická válka již začala (např. Geers 2013, Martínez 2013), stejně jako že kybernetická válka ani nastat fakticky nemůže (Rid 2013). Zatímco Martínez (2013) považuje za kybernetickou válku sérii aktuálních špionážních aktivit a celosvětové rozšíření APT[36], Rid (2013) ji naopak probírá z pozice čisté clausewitziánské války. V prvním případě je za kybernetickou válku označován stav, který nemá s bezpečnostně-vědním pojetím války mnoho společného, v případě druhém pak její rigidní chápání zabraňuje myslet mimo mantinely tradičních domén válečnictví a znemožňuje tak řádně domýšlet důsledky rozšíření informačních a komunikačních technologií ve společnosti. Thomas Rid (2013) se proti míchání pojmů kybernetické války a kybernetického válčení ostře ohradil v knize Cyber War Will Not Take Place a ač nelze souhlasit s mnoha jeho závěry, je nutné mu přiznat, že přesvědčivým způsobem vymezuje, proč nelze (minimálně v současné době) hovořit o probíhající kybernetické válce.

Podíváme-li se přímo na nabízené definice, pak například Clarke a Knake (2010: 6) definují kybernetickou válku jako aktivity národního státu s cílem proniknout do počítače a sítě jiného národa se záměrem způsobit škodu nebo určité rušení. Podobným směrem se ubírá i Healey (2013: 281), který však přidává prvek závažnosti. Jedná se o [...] „*jednání národního státu s cílem poškodit nebo rušit počítače a sítě jiného národa, které způsobuje značné poškození nebo ničení – efekty podobné jako při použití tradiční vojenské síly – a je proto považováno za ozbrojený útok. Národ v kybernetické válce je de facto v opravdové válce, což znamená, že v reakci na takový útok může použít smrtící sílu.*"[37]

Lachow (2009: 441) pak kybernetickou válku vymezuje dle Arquilla a Ronfeltd (1997) spíše z hlediska vojenských aspektů soupeření. *„Kybernetická válka odkazuje*

[35] Například Libicki (2009) používá termín kybernetická válka (cyberwar) ve smyslu způsobu vedení války (warfare). Podobně tak činí i Bastl, který kybernetickou válku pojímá jako páteř subtypu informační války (Bastl 2007: 78).
[36] APT neboli Advanced persistant threat – jedná se o útok, jehož účelem je typicky dlouhodobě infiltrovat a zneužít cílového systému nebo jeho dat za pomoci pokročilých, adaptivních a sociálně-technických metod (srov. Jirásek a Novák a Požár 2013).
[37] Překlad autora této práce.

k provádění a přípravě vojenských operací v souladu s principy informačního válečnictví. To znamená narušení, pokud ne přímo zničení informačních a komunikačních systémů, široce definované tak, aby zahrnuly i vojenskou kulturu, na které protivník závisí [...]"[38]

Valeriano a Maness (2014) pak souhlasí s Ridem (2013), když odmítají pojem kybernetické války, jelikož je dle nich velice nepravděpodobné, že se ve svém nejzazším smyslu, kdy dochází ke smrti jedinců, objeví. Při odkazu ke Gartzkeho (2013) chápání kybernetické války jako prostředku států k vedení konfliktů nízké intenzity pak Valeriano a Maness (2014) uzavírají, že je spíše nutné nahlížet na tento fenomén jako na kybernetické konflikty a to právě z důvodů nemožnosti projevení násilí s takovými efekty, jaké vyžadují clausewitziánské definice války.

Singer a Friedman (2015: 121) k tomuto poznamenávají: *„Hranice kybernetické války mohou být stejně tak nejasné: ‚My, ve Spojených státech, máme tendenci uvažovat o válce a míru jako o jednoduchém přepínači zapnout-vypnout – jako válce v plném rozsahu nebo období míru' říká Joel Brenner, bývalý šéf kontrarozvědky pod ředitelem Národní zpravodajské služby. ‚Realita je odlišná. Nyní jsme v konstantním konfliktu mezi národy, který se zřídka vyvine v otevřenou válku ... Musíme si zvyknout na to, že i země jako je Čína, se kterou jistě nejsme ve válce, jsou s námi v intenzivním kybernetickém konfliktu.'"*[39] Tento komentář Joela Brennera je snad namířen proti míchání pojmů nejen v rámci bezpečnostní komunity, ale i vně směrem k širší veřejnosti.[40]

Kybernetická válka je tedy vesměs definována v souladu s bezpečnostně-vědním chápáním války dle Moellera (2004) či Šmída (2010), ač bez kvantitativního požadavku na počet obětí. Kybernetickou válkou se proto rozumí stav, kdy státy vyvíjí aktivity ke zničení nebo narušení počítačů nebo sítí jiného státu, což by mělo za následek těžké

[38] Překlad autora této práce.
[39] Překlad autora této práce.
[40] Je možné spekulovat, do jaké míry hraje v nadužívání pojmu ‚válka' svou roli neznalost a do jaké míry určitý aktivizační sentiment v rámci komunity. Nazveme-li určitou situaci válkou, dostane se jí obvykle daleko větší pozornosti z širokého okruhu oblastí. Válka proti terorismu nebyla válkou v pravém slova smyslu, nazvání postupu vlády Spojených států proti zamezení fungování a aktivit teroristických skupin však pomohlo k sekuritizaci této problematiky natolik, že byla (a do jisté míry stále je) velkým tématem vnitřní bezpečnosti Spojených států dodnes.

ztráty v důsledcích podobné, jako kdyby byly dosaženy konvenčními silami.[41] Kybernetická válka je de facto vždy klasickou mezistátní válkou, avšak vedena zejména prostřednictvím kyberprostoru.

Na jedné straně autor této práce souhlasí s Ridem (2013), který odmítá nadužívání pojmu ‚války' v této diskuzi, na straně druhé se však nedomnívá, že by taková válka nemohla nastat. Pokud by však nastala, byla by pouze jednou z oblastí války obecné podobně, jako je tomu u vzdušné, námořní či pozemní války. V tomto smyslu by pak tento pojem byl vlastní spíše výzkumu válečnictví.

2.6. Další blízké fenomény

V souvislosti s kybernetickými konflikty, válkou a válečnictvím v rámci kyberprostoru je vhodné věnovat místo i stručnému přehledu a vymezení dalších fenoménů, které se k nim váží. Jejich pojetí může pomoci lépe podchytit jednotlivé incidenty a případně popsat či zasadit části jejich okolností.

2.6.1. Hacktivismus

Hacktivismus je spojením aktivismu a hackingu. Aktivismus v kyberprostoru odkazuje na jeho normální používání, které nenarušuje jiné systémy, s cílem podpořit určitý záměr nebo agendu (Denning 2001), zatímco hacking je termín označující aktivity vedoucí k narušení zabezpečení ochrany programu nebo systému s cílem do něj proniknout (srov. Jirásek a Novák a Požár 2013). Hacktivismus tak pojímá operace, které využívají hackerské techniky proti určitému cíli připojenému (nejen) k Internetu s cílem narušit běžné operace, avšak nezpůsobující výraznou škodu (Denning 2001). Příkladem takového jednání pak jsou webové protestní akce, virtuální blokády, automatizované emailové bomby, hackování webů, neoprávněné přístupy do počítačů apod. (Tamtéž). Slovník kybernetické bezpečnosti (Jirásek a Novák a Požár 2013) zdůrazňuje dosažení politických cílů nebo podporu politické ideologie, Singer a Friedman (2014) pak přidávají diskutabilní otázku legálnosti hacktivistických aktivit a zejména nenásilnost aktivit, nesměřující ke zranění či zabití představitelů opozitního aktéra, kdy jde stále o jakousi formu aktivního protestu, nikoli letálního boje.

[41] Takové aktivity je pak možné považovat za ozbrojený útok i z mezinárodněprávní perspektivy.

2.6.2. Kybernetické povstalectví

Ke konceptu kybernetického povstalectví se vyjadřuje Drmola (2014), který považuje v současné teorii přítomné koncepty hacktivismu a kybernetického terorismu za velmi vzdálené, co se týče závažnosti jím vlastních politicky destruktivních aktivit. Z tohoto důvodu přichází, podobně jako ve fyzickém světě, s konceptem kybernetického povstalectví.

Oproti kybernetické kriminalitě jsou cíle politické, nikoli zaměřeny na zisk. Oproti kybernetické válce se dle něj jedná o vysoce asymetrický fenomén a zároveň zahrnuje určitou kontrolu populace. Kybernetickému povstalectví je vlastní i zpochybňování současných autorit, stejně jako kontrola nedostatečného množství finančních prostředků, kontroly médií vládní nebo zákonodárné moci apod. Následuje určitou logiku hacktivismu, avšak zatímco činy hacktivistů jsou vesměs „pouze“ narušující, v rámci kybernetického povstalectví jsou dané aktivity daleko závažnější, destruktivní a smrtelné. Dodává však, že v současné době se kybernetické povstalectví nevyskytuje, ač nelze do budoucna vyloučit (Drmola 2014).

2.6.3. Kyberterorismus

Kyberterorismus je kategorií škodlivých aktivit svého druhu. Na škále snahy o dosažení určitých politických cílů je jej možné považovat za nejextrémnější fenomén, který se nezaměřuje pouze na útok proti vládnímu režimu, ale útočí (ať již násilně nebo zastrašováním) také na široké obyvatelstvo (Drmola 2014). Denning (2001) uvádí, že podobně jako u hacktivismu, i zde se jedná o spojení dvou fenoménů, a to kyberprostoru a terorismu. Následně jej popisuje jako politicky motivované hackerské operace s cílem způsobit závažnou újmu, jako ztrátu na životech nebo závažnou ekonomickou škodu. Jako příklad pak uvádí penetraci do systému řízení letového provozu a přinucení dvou letadel se srazit. Je však nutno podotknout, že existuje mnoho rozporů ohledně přístupu k tomuto konceptu – někteří jej vnímají situaci, kdy teroristické skupiny pro svou hlavní činnost využívají i možnosti, které jim poskytuje kyberprostor – ty však samy o sobě často nemusí plnit základní definice terorismu, tj. např. šíření strachu mezi populací, použití nebo hrozba použití násilí apod. V rámci tohoto pohledu se někteří domnívají, že je kyberterorismus jen teoretickým konceptem, který de facto ani existovat nemůže (Flook 2009).

2.6.4. Kyberkriminalita

Kyberkriminalitou se obvykle rozumí trestná činnost páchána prostřednictvím kyberprostoru. Slovník kybernetické bezpečnosti (Jirásek a Novák a Požár 2013: 57) ji definuje následovně: *„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“*

Kyberkriminalita se může dělit na několik druhů, a to (i) trestné činy proti kyberprostoru samotnému (tj. schopnosti jeho fungování), (ii) trestné činy, které nemíří proti kyberprostoru samotnému, ale lze je spáchat pouze v tomto prostředí (příkladem může být neoprávněný přístup do systému nebo k datům apod.), (iii) trestné činy, které jsou s kyberprostorem relativně pevně spojeny, avšak objekt zájmu ochrany je odlišný (např. počítačové pirátství jako forma porušení ochrany duševního vlastnictví) nebo také (iv) klasické trestné činy spáchané převážně prostřednictvím kybeprostoru (příkladem zde mohou být obyčejné podvody pomocí phishingových emailů, které využívají důvěřivost příjemců těchto zpráv).

Vztah kybernetické kriminality a kybernetického konfliktu je opět velmi specifický. Sama o sobě nemá politický podtext. V kyberprostoru nicméně často nelze rozeznat obecný cíl útočníka, kdy na straně napadeného může vzniknout dojem, že se jedná o politicky motivované aktivity. Stejně tak mohou být najímáni jednotlivci nebo organizované kriminální skupiny k páchání kybernetických útoků k dosažení politických cílů[42] jiných subjektů.

2.6.5. Klasický hacking

Klasickým hackingem je zde rozuměn fenomén existence a aktivit osob s výjimečnými znalostmi a talentem, který využívají pro překonávání zabezpečení informačních a komunikačních systémů jiných subjektů, avšak bez specifických motivací. Jejich hlavní motivací není prospěch či poškození druhé strany, ale získání vědomostí, dalších zkušeností a snad i věhlasu, které jiným způsobem nebyli možní získat. Tento koncept

[42] Příkladem budiž kybernetický útok na Gruzii v roce 2008, při kterém byla k provedení části útoků s největší pravděpodobností najata kriminální skupina Russian Business Network. Viz dále v této práci.

je použit ve shodě s definicí Roba Sheina (2010). Role klasických hackerů a jejich možný vliv na konflikt je popsána níže v této práci.

2.6.6. Patriotický hacking

Tikk a Kaska a Vihul (2010) při analýze právních dopadů útoků na Estonsko v roce 2007[43] představují koncept patriotického hackingu, který je již relativně dlouho, ač ne příliš hojně, v oblasti kybernetické bezpečnosti užíván (viz např. BBC 2003, Leyden 2013 nebo Kumar 2012). Patriotický hacking odkazuje k zapojení občanů do kybernetických útoků vedených vůči určitému vnímanému protivníkovi svého státu (např. jinému národu). *„Jako takový, patriotický hacking je prováděn skupinou lidí, kteří podnikají kroky pro zájmy své země v případech, kdy věří, že jejich akce je ta správná věc pro jejich vládu nebo tam, kde se domnívají, že vláda není schopna učinit ‚správnou věc'"*[44] (Tikk a Kaska a Vihul 2010: 31). Uvedené autorky poté tento termín diskutují zejména z právního hlediska, nicméně i z hlediska bezpečnostních studií má svůj význam.

Svým popisem může do jisté míry připomínat hacktivismus, nicméně oproti obyčejnému hacktivismu je obvykle v souladu s postoji země, ke které je útočník loajální, a dále je také neutrální vzhledem ke způsobu útoků. Patriotický hacking tedy nemusí být pouhým relativně málo škodlivým útokem – naopak může způsobovat škody velké, ať již způsobené omezením poskytování služeb, krádežemi dat apod. Tento typ útoků je i relativně nebezpečným z hlediska přístupů států k němu, kdy právě využití takových hackerů může být velmi účinným prostředkem k částečnému prosazování svých cílů. Stát nemusí takové aktéry materiálně podporovat či dávat příkazy k provádění jednotlivých akcí; stačí pouze vytvořit správný sentiment ve společnosti, která takovému sentimentu lehce podlehne. Aktéři pak již jednají samostatně, nikoli řízeni státem. Důsledkem je nulová přímá právní odpovědnost zdrojového státu; sekundární odpovědnost v rámci due dilligence nebo při následném kriminálním stíhání je již velmi obtížně aplikovatelná a nezřídka se stává, že nejsou za takové útoky vyvozeny žádné sankce, ať již mezinárodně-právní či kriminální (srov. Tikk a Kaska a Vihul 2010).

[43] Vizte níže v této práci.
[44] Překlad autora této práce.

3. Výzkum kybernetických konfliktů

Po vymezení pojmů vážících se ke kybernetickému konfliktu je také vhodné nahlédnout na zásadní specifika kybernetického konfliktu v jednotlivých konfliktních atributech. Níže uvedené charakteristiky a komentáře k daným atributům nelze považovat za vyčerpávající, jedná se spíše o zdůraznění některých zvláštností, které se v daném rámci vyskytují.

3.1. Aktéři

Pšeja (2002) souhlasí s Holsti (1983), když tvrdí, že konflikt je střet mezi jasně definovatelnými aktéry (Zeman 2002: 52). Jak však lze vidět, Healey (2013) tento požadavek na určitost aktérů nemá; v jeho definici je dostačující fakt, že zde aktéři existují. Je otázkou, zdali určitost Healey vynechává záměrně; taková definice de facto připouští existenci konfliktu s neurčitým, popřípadě i s neznámým aktérem. Jak již bylo uvedeno výše v této práci, neurčitost aktérů a obtížnost přisouzení některých škodlivých aktivit činí oblast kybernetických konfliktů velmi specifickou. V mnoha případech lze dojít k situaci, kdy zde v rámci širší kampaně existuje útok, cíl útoku a jeho škodlivý následek, nicméně není možné přesvědčivě určit původce útoku. Vše pak zůstane pouze na větší či menší míře jistoty, který aktér přesně provedl ten který útok.

Sám Healey (2013: 21) se vyjadřuje, že neurčitost aktérů nemusí být problémem – i přesto, že některé kybernetické útoky je technicky velmi obtížné přisoudit, nemusí to být při hledání zodpovědného aktéra konečná. Takové útoky se totiž pravidelně odehrávají v rámci probíhajících geopolitických krizí a určení zodpovědného národa (strany) tak bývá relativně přímočaré.

Na jedné straně je pochopitelné, že nelze-li pachatele útoku odhalit přímými důkazy, pak je nutné použít dobře vyargumentované důkazy nepřímé. To však vytváří značný prostor pro chyby strategického významu. Když se v únoru 1998 zvyšovalo napětí v Perském zálivu a Spojené státy zde vyslaly množství svých jednotek, bylo zjištěno závažné narušení bezpečnosti informačních systémů amerického letectva kybernetickým útokem, který byl vystopován až ke Spojeným arabským emirátům, které byly jednou z mála zemí, skrze kterou byl Irák napojen do internetové sítě. Některými představiteli byl útok popisován jako do té doby nejorganizovanější a nejsystematičtější útok na sítě Pentagonu. Vzhledem ke známým okolnostem tedy bylo

logickým závěrem, že byl za tímto útokem Irák a v kyberdoméně tak již skutečně započaly válečné kampaně (Maurer 2013). O několik týdnů později hlubší vyšetřování odhalilo, že za útokem stáli dva teenageři z Kalifornie za pomoci dalšího mladíka z Izraele. Útok neměl politický podtext, nebyl ani proveden s úmyslem ukrást či poškodit nějaká data – pro hackery bylo dostačující, že se jim podařilo získat přístup do citlivých vládních systémů a tím získat určitou trofej a dobrý pocit ze svých schopností (Tamtéž).

Načasování v rámci širší politické krize a zároveň zapojení izraelského mladíka však vyvolalo mylnou představu, která mohla být naprosto zásadní. Bez ohledu na skutečný pozdější vývoj v regionu mohl tento závěr započít ozbrojený konflikt v tom ohledu, že by byl považován za součást širší vojenské operace nepřítelem. Lze dodat, že kontext, ve kterém byl útok proveden, nebyl úmyslně zvolen a i náhoda a „správné“ načasování zde sehrálo svou roli. Stále je pravděpodobnější, že probíhající kybernetický útok lze dát do souvislosti s širším geopolitickým kontextem a proto je možné s jistou rezervou s Healym souhlasit. Jeho přístup však nelze brát jako zlaté pravidlo, a to tím víc, že nemožnost dohledat a konkrétně určit útočníka je v historii kybernetických konfliktů i relativně dobře zaznamenána (Arquilla 2013).

Problematika přičitatelnosti aktivit v kyberprostoru je velmi obsáhlá. Na tomto místě je cílem poukázat na jednu ze slabin teorie kybernetických konfliktů – konflikt lze řádně analyzovat tehdy, když známe motivace aktérů, k čemuž je někdy nutné znát aktéra samotného. Operace v kyberprostoru nemusí být natolik přímočaré jako ozbrojené útoky v reálném světě. Zjištěné napadení informačních či komunikačních systémů může mít různé efekty, které v době napadení či odhalení nemusí být oběti známy. Zatímco pro útočníka může mít kybernetický útok pouze čistě ekonomický (kriminální) podtext, na straně oběti může vzniknout percepce útoku jako politicky motivovaného, který vyjadřuje postoj pravděpodobné strany a tím mít podstatný dopad na dynamiku i jiného paralelně existujícího konfliktu. Taková situace není v bezpečnostní oblasti úplně nová – i při konvenčních ozbrojených konfliktech je možné provést akci tak, aby byla přisouzena jinému subjektu. V kyberprostoru je však tato možnost daleko větší a významnější, a to i vzhledem k množství aktérů, kteří zde operují.

Tento problém se velmi řeší v oblasti mezinárodního práva a bezpečnostní politiky (viz např. Schmitt a Vihul 2014). Zde však existuje do jisté míry praktické (leč někdy

nepříliš efektivní) řešení v podobě aktivace pasivní odpovědnosti státu, v jehož jurisdikci leží infrastruktura použitá ke kybernetickému útoku[45] (např. Deeks 2013). U zkoumání kybernetických konfliktů toto není možné – jejím hlavním smyslem totiž není určit efektivní a spravedlivou odpovědnost za útok k jeho zabránění, jako spíše zjistit skutečný stav věci, skutečné aktéry a skutečné motivace. Nejen z výše uvedeného tak je výzkum kybernetického konfliktu nucen čelit výzvě, kterým je obtížnější zjišťování zdrojů útoků a motivace aktérů.

3.2. Oblast střetu

Pokud při zkoumání určíme s nižší či vyšší mírou pravděpodobnosti aktéry útoků, jsme pak také schopni určit jejich motivace a zejména oblast střetu. V tomto ohledu se pak kybernetické konflikty nijak významně neliší od obecné teorie konfliktu. Oblastí střetu se totiž rozumí zejména různé hodnoty či zájmy aktérů, které pouze skrze kyberprostor prosazují. Kyberprostor sám o sobě je cílem pouze výjimečně; v drtivé většině jsou pouze přes něj při konfliktech artikulovány a prosazovány jiné širší politické cíle, které mohou být vyjádřeny i mimo něj. Pokud cílem je, pak zejména specifickým[46] v takovém rámci, v jakém chápe kybernetický útok např. Hathaway (2012) (viz výše), tj. cílem vojenským, na který aktér útočí a snaží se jej poškodit. Takové poškození je opět zpravidla součástí širšího politického cíle.

Zjištění oblasti střetu při výzkumu kybernetického konfliktu může být opět velmi obtížné z důvodu zakrývání skutečného cíle jednání jednotlivých aktérů. V případě výše uvedeného proniknutí do systémů Pentagonu za období krize v Perském zálivu nebylo možné de facto nic říci o motivech útočníků, než byli dopadeni. Lze také uvést rozsáhlé DDoS útoky na Českou republiku v roce 2013 zaměřené na zpravodajské servery, bankovnictví či mobilní operátory. Ač měly potenciál způsobit určité škody, nestalo se

[45] Základem této odpovědnosti je tzv. princip „due dilligence“ neboli řádné bdělosti státu, který má povinnost zabezpečit, aby nebyly z jeho území prováděny nepřátelské aktivity vůči jinému subjektu mezinárodního práva. Více viz Schmitt eds. (2013).

[46] Specifické cíle aktérů mohou být na kyberprostoru velmi závislé a významně se mění vzhledem k charakteru konfliktu; tak například u vyspělé země závislé na informačních a komunikačních technologiích bude defacement jejich nejzásadnějších portálů účinnější, než u země, kde rozvoj veřejných služeb skrze kyberprostor je teprve na začátku. Zde by pak byla daleko racionálnějším způsobem snížení morálky protivníka např. letáková kampaň, popřípadě jiná forma klasické neelektronické propagandy. Je pak však otázka, do jaké míry je specifický cíl cílem z pohledu výzkumu konfliktu, a do jaké míry je cílem z hlediska vojenství a způsobu vedení konfliktu. Jinými slovy – cílem obecným je nějaký vyšší zájem nebo hodnota, kterou teprve pomocí narušení kyberprostoru aktér dosahuje. Pouze teoreticky je možné uvažovat situaci, kdy by hlavním cílem byl kyberprostor samotný (srov. Drmola 2013: 24).

tak, a jelikož se k útoku nepřihlásil žádný aktér (a ani žádný konkrétní nebyl dohledán), nebyl nalezen skutečný důvod těchto útoků. Vzhledem ke kontextu se spekuluje o tomto útoku jako testovacím (např. Kreč a Klang 2015), kdy byly systémy České republiky využity pro vyzkoušení určitých metod útoků, které mohou být následně použity proti zemím s větší strategickou významností.[47] To však opět zůstává v rovině (kvalifikovaných) odhadů a pravděpodobností, s jistotou nebylo možné úmysl a (širší) cíl aktéra zjistit. Healyho (2013) přístup v posouzení aktuální geopolitické situace a kontextu útoků stále zůstává nejpoužitelnějším řešením této situace.

3.3. Napětí

Podobně je na tom i složka napětí, která je v případě kybernetického konfliktu přítomna. Napětí samo o sobě je tvořeno pocity a postoji aktérů kvůli neslučitelnosti zájmů nebo hodnot, které zpravidla bývají nezávislé na existenci či neexistenci kyberprostoru. Kyberprostor jako specifické prostředí lidských interakcí však může mít zvláštní vliv projevy napětí. Svou přístupností a částečnou anonymitou poskytuje kyberprostor možnost jak napětí projevovat daleko snáze než by bylo možné v čistě fyzickém světě.

Na kyberprostor však nelze nahlížet pouze jako na katalyzátor dynamiky konfliktu; podobně může mít i inhibiční účinky. Důvodem je zejména užívání kyberprostoru jako zdroje informací. Existují-li informace, které napětí zvyšují, mohou existovat také informace, které přispívají k jeho snížení. Vlastnost kyberprostoru jako prostředí umožňujícího komunikaci a výměnu informací z něj činí platformu s dopadem na konfliktní napětí. Konfliktní napětí při kybernetickém konfliktu je pak možné ovlivňovat například podle míry kontroly kyberprostoru (např. státem) nebo naopak absencí kontroly a ponechání obsahu v rukou jednotlivců.

Samotná složka napětí je však stále vlastní jednotlivým aktérům konfliktu a její charakter ji spojuje s postoji daných aktérů. Napětí není vytvářeno a uchováváno v kyberprostoru, to je vlastní racionalitě či iracionalitě (viz Bartos a Wehr 2002) aktérů samotných.[48]

---

[47] Více viz např. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.

[48] Existují zde i určitá východiska, jak se pokusit napětí lépe analyzovat. Například Valeriano a Maness (2014) se při zkoumání kybernetického konfliktu zaměřují na rivalitu mezi populacemi jednotlivých území, než na interakce mezi jednotlivými státy. *„Koncept rivality přináší zpátky do výzkumu politických věd historii a znaky interakcí. Pro pochopení, proč se rozvinuly krize*

3.4. Jednání

I na jednání lze pohlížet v kontextu výše uvedeného – kyberprostor ovlivňuje jeho pravděpodobnost, rozšířenost i závažnost vzhledem k relativní jednoduchosti a snadnému přístupu k veřejným sítím elektronických komunikací. Aktivity mohou být jak donucovací (zejména kybernetické útoky), tak nedonucovací (např. aktivizační nástroje kybernetické propagandy), násilné i nenásilné, atd.[49] Aktéři pak ke kyberprostoru přistupují podobně jako k jakékoli jiné doméně (prostředí) střetu, snažící se využít její příležitosti a také slabiny.

Mezi speciální vlastnosti kyberprostoru, ovlivňující možnosti skrze něj jednat, lze zařadit zejména (i) dostupnost kyberprostoru z různých částí světa, díky kterému je možné se přihlašovat k jednomu systému téměř odkudkoliv. Dále (ii) rozšířenost využívání informačních a komunikačních technologií připojených do veřejných sítí, díky čemuž je takových systémů celá řada, poskytující a ovlivňující nepřeberné množství aktivit. Kyberprostor je také velmi (iii) komplexní – jednotlivé komunikační a informační systémy nejsou na sobě vždy nezávislé, a výpadek či narušení jednoho systému, může způsobit výpadek či narušení druhého. Podobně je kyberprostor i (iv) komplikovaný, kdy jeho detailní fungování vyžaduje odborné znalosti; na straně druhé však jeho běžné užívání je (v) triviální a je proto přístupný širokému počtu jedinců. V neposlední řadě může mít na jednání vliv i (vi) virtuálnost kyberprostoru a navazující psychologické faktory ovlivňující chování jedinců v něm (např. pocit anonymity), a (vii) s tím související aktivizační potenciál, kdy je skrze kyberprostor možné dodat velkému množství jedinců mnoho informací ve velmi krátkém čase (srov. Libicki 2009, Choucri a Goldsmith 2012).

Tyto atributy nejsou v žádném případě vyčerpávající, mohou však být zásadní pro správné uchopení problematiky kyberprostoru a konfliktu. Jejich správné zhodnocení je totiž často jediným základem a odrazovým můstkem. Zatímco aktéři mohou zůstat skryti, jednání je vždy projevováno směrem navenek.

---

nebo války, je třeba na historii interakcí na vojenských, diplomatických, sociálních a kulturních úrovních (Valeriano 2013). Rivalita je pak definována jako dlouhotrvající konflikt s přetrvávajícím nepřítelem (Diehl & Goertz 2000)"

[49] Násilnost konfliktního jednání v kyberprostoru je v současnosti značně omezena i přesto, že není vyloučena a existuje zde předpoklad na růst možností jednání s efekty podobnými jako při násilném jednání.

U konvenčních konfliktů bereme při zhodnocení daného problému relativně omezenou množinu možných aktérů a omezenou množinu jednání, která mají směřovat k prosazení jejich cíle. U kybernetického konfliktu je nutné daleko více brát v potaz skutečnost, že mnoho jednání ovlivňujících situaci není (v určitý moment) viditelných, stejně jakože množina pravděpodobných aktérů a jejich cílů je nepoměrně širší než při konvenčním konfliktu. Zatímco při raketovém útoku na vojenskou základnu je velmi rychle znám specifický cíl, který daleko více zmenšuje množinu možných politických cílů, stejně jako je znám způsob útoku, který ve spojení s teritoriálním ukotvením dává lepší odhad o původci útoku, v rámci kybernetického konfliktu je velice obtížné si být jistý i téměř „jasně vypadajícími" útoky. Naopak velmi podobně se jeví odkaz ke komplikovanosti a zároveň triviálnosti technologií – sestrojit sofistikovanou zbraň vyžaduje jistou odbornost a zdroje, její užití již však může být velmi triviální.

Není na tomto místě možné debatovat veškeré specifika, které je při výzkumu kybernetických konfliktů nutné vzít v potaz; spíše se práce snaží o představení problematiky (a problematičnosti) této činnosti. Kybernetický konflikt je fenoménem, který si zaslouží pozornost i v rámci konfliktologie; z tohoto důvodu a právě pro její problematičnost je však nutné jednak operovat s přesnou terminologií a s uvážením hlavních specifik, které tento fenomén má.

K uzavření této části, P.W. Singer a Allan Friedman (2014) popisují pomocí vyjádření Michaela Haydena, bývalého ředitele CIA, důležitost správných informací a znalostí o fungování kybernetického prostoru: *"Jen vzácně bylo diskutovaného něco natolik důležitého s tak malým pochopením ... seděl jsem na velmi malé skupinové poradě ve Washingtonu ... neschopný (společně s mými kolegy) rozhodnout o dalším postupu, protože nám chyběl jasný obrázek o dlouhodobých právních a politických dopadů jakéhokoli rozhodnutí, které jsme mohli přijmout"*[50] (Singer a Friedman 2014: 4). Ač je znalost problematiky kybernetických konfliktů v současné době nejen u politických představitelů stále malá, Jason Healey (2013) to nepřičítá pouze překotnému vývoji informačních a komunikačních technologií, přičítá to i špatnou schopností udržet znalost této problematiky mezi politickými představiteli.

[50] Překlad autora této práce.

4. Stanovení objektu, cílů a oblastí analýzy

Záměrem následující části práce je se orientovat na kybernetické konflikty v post-sovětském prostoru. Důvodů pro výběr této oblasti je několik. Jednak význam kybernetického prostředí v rámci prosazování politických cílů vzrůstá – vzhledem k dnešní roli Ruské federace, její bezpečnostní politice a vůbec vnímání své bezpečnosti ve vztahu k sousedním zemím[51] může být užitečné popsat a analyzovat vedle sebe nejdiskutovanější případy narušení kybernetické bezpečnosti v její sféře vlivu a popřípadě se pokusit zjistit společné znaky či trendy, které se zde objevují. Zajímavým společným bodem předmětných kybernetických útok je skutečnost, že se odehrály na pozadí jiných v té době probíhajících konfliktů či sporů v rámci regionu[52] a vyznačovaly se omezením poskytování služeb, popř. defacementy, zahlcením sítí apod. Nejednalo se tak o (de facto neustále probíhající) skryté zpravodajské či špionážní aktivity, ale aktivity směřující k narušení fungování služeb, popřípadě přímo ke způsobení určité škody a (přinejmenším obětí vnímané) donucení protivníka jednat v reakci na daný útok.

Případy jsou vybrány také dle jejich diskutovanosti v odborných kruzích a „zřejmosti" jejich konfliktní povahy. Časový rámec je uvozen roky, ve kterých ke sledovaným incidentům došlo. Jejich výběr je dán i jejich charakterem, zejména když nelze předpokládat, že by byly jednotlivé kybernetické útoky ve svém souhrnu pouze kriminálními aktivitami bez širších politických cílů.

Analýza jednotlivých konfliktů se vedle úvodního popisu zaměří na kontext útoků, dále popíše útoky samotné včetně jejich cílů, způsobů a popř. aktérů a událostí odehrávající se po nich. Tyto oblasti jsou vybrány z relativně prostého důvodu – při analýze konfliktů s pravděpodobně skrytými aktéry je nutné vyvozovat závěry i z množství nepřímých důkazů. Pouze analýza relevantních souvislostí, které jsou zdokumentované, může mít své opodstatnění. Zaměřili-li bychom se jen na určitou část (např. cíle, způsoby a dopady), neposkytlo by nám to zasazení incidentů do tolik potřebného širšího rámce.

[51] Vizte níže kapitolu 6. této práce.

[52] Nejednalo se o APT či jiné dlouhodobé špionážní nebo útoky využívající záměrně vytvořených zadních vrátek na software nebo hardware.

V rámci kontextu se pak práce pokusí nastínit vztah napadené země a Ruské federace, a poté se zejména zaměřit na události, které útokům bezprostředně předcházely. V tomto rámci pak představí (údajný) spouštěč útoků, podobně zde bude přiměřeně věnována pozornost i dalším možným souvislostem.

Cíle útoků jsou dalším bodem analýzy; v této části se analýza zaměří na specifické cíle útoků, tj. zdali byly zaměřeny na veřejný nebo soukromý sektor, a popřípadě jaké služby byly útoky zasaženy. V části způsoby útoků pak práce stručně popíše prostředky, které byly při jednotlivých útocích použity, a to zejména ve formě jednotlivých druhů útoků, ať již defacementy, DoS nebo DDoS útoky a jiné. Práce se také pokusí popsat rozsah a komplexnost jednotlivých útoků a závažnost jejich dopadů. V rámci aktérů se pak pokusí práce analyzovat jednotlivé aktéry daného konfliktu, jejich charakter, původ, jejich politické či jiné cíle apod. Nebude zde však snaha dosvědčit přímou odpovědnost aktérů za provedené útoky.

Nakonec práce analyzuje zmíněné konflikty i ve smyslu jejich dopadů, a to jak ve smyslu dopadů vnitřních v rámci aktéra zasaženého útoky, tak případně i mezinárodně-politických.

Výstup těchto analýz bude použit pro diskuzi nad kontextem útoků, útoky samotnými a obecným konfliktem, který v jejich rámci existoval.

5. Kybernetické konflikty

5.1. Estonsko 2007

5.1.1. Kontext

Estonsko je relativně malou zemí na pobřeží baltského moře, která sousedí s Lotyšskem na jihu a Ruskou federací na východě. Zároveň se nachází velmi blízko jazykově a kulturně spřízněnému Finsku. Tato geografická pozice do jisté míry předurčila i historii Estonska. První nezávislosti dosáhlo Estonsko v období konce první světové války, do které bylo součástí Ruského impéria. Tuto nezávislost však opět ztratilo sovětskou okupací za druhé světové války v rámci rozdělení sféry vlivu v Evropě paktem Molotov-Ribbentrop (Plakans 2011). V období po druhé světové válce pak bylo Estonsko jednou ze sovětských republik a to až do 90. let, kdy se Sovětský svaz postupně rozpadl.

Nově nabytá nezávislost byla vyhlášena dne 20. srpna 1991, kterou Sovětský svaz sám uznal dne 6. září 1991. Od této doby se Estonsko snažilo o větší sepjetí se zeměmi západní Evropy, což bylo potvrzeno v roce 2004 vstupem Estonska do NATO a Evropské unie. Estonsko se tak stalo de facto součástí euroatlantické části světa, avšak stojící na její bezprostřední hranici s dějinným oponentem.

Díky historickému sepjetí s Ruskou Federací se v Estonsku nachází početná ruská menšina. V současné době je odhadováno, že se jedná až o téměř čtvrtinu populace celé země. Etničtí Rusové nejsou do estonské společnosti integrováni rovnoměrně; část drží estonské občanství, hovoří estonsky a považuje Estonsko na svou zemi, část jsou občany Ruské federace, nicméně stále uznává ústavní pořádek země, a část považuje rozpad SSSR za chybu a přeje si znovu obnovení ruské kontroly nad Estonskem (Tikk a Kaska a Vihul 2010: 15). Rusové navíc nejsou rozprostřeni po celé zemi rovnoměrně, většina etnických Rusů je přítomných v hlavním městě Tallinnu a severovýchodních částech státu. Estonsko bylo také několikrát obviněno z porušování lidských práv a diskriminace této menšiny (Elsuwege 2004).

Mezi Estonskem a Ruskem se v novodobé historii objevila řada sporů, a to vesměs ideologických. Estonsko bylo několikrát obviněno ať již oficiálními představiteli Ruska, nebo dokonce i zpravodajskými komentátory, z honorování nacistického režimu ve vztahu k pomníku estonského vojáka bojujícího v období druhé světové války proti

Sovětskému svazu (BBC 2002, The Economist 2007a). Zatímco Estonci vidí období sovětské nadvlády jako symbol okupace, Rusové je berou jako osvobození a aktivity, které tento pohled narušují, vyvolávají značné emoce (BBC 2005). Vedle toho se objevily mezi těmito státy i některé další teritoriální spory.

Oproti mnoha jiným státům se Estonsko relativně dobře popasovalo s přeměnou na prosperující liberální stát. S pouhými cca 1,3 miliony obyvatel, limitovanými zdroji a nízkou hustotou populace bylo nuceno hledat způsoby, jak poskytnout obyvatelstvu veřejné služby při vynaložení minimálních prostředků (Tikk a Kaska a Vihul 2010: 16). Stejně tak bylo nutné učinit Estonsko konkurenceschopné v nově nastoleném mezinárodním prostředí. Z tohoto ohledu pak učinilo velmi zásadní krok, když byl v polovině 90. let nastaven důraz na rozvoj a využití informačních a komunikačních technologií, které pomáhaly těmto výzvám úspěšně čelit. Této podpory vlády nejprve využily banky, později i další subjekty soukromého sektoru (Tamtéž). Základy elektronizace veřejné správy byly položeny v letech 2000 až 2002, kdy byl přijat zákon o využívání informačních technologií ve veřejné správě – elektronické operace tak byly z hlediska správního práva postaveny na stejnou úroveň jako úkony písemné. To zároveň vyžadovalo rozšíření nutných technologií mezi nejširší obyvatelstvo, včetně elektronického podpisu (Tamtéž).

Do roku 2007 byly státní informační systémy a databáze propojeny do jednotného informačního systému s vlastní specifickou infrastrukturou. Jeho součástí bylo na 150 informačních systémů veřejného sektoru s více než 1000 různých elektronických služeb. V roce 2005 se stalo Estonsko první zemí světa, které volilo zástupce do veřejných funkcí přes internet (Euractiv 2007).[53] Využívání ICT soukromou i veřejnou sférou se v současnosti na přímých nákladech šetří okolo 2% HDP ročně (Luht 2014).[54] Estonsko se tak postupně stalo zemí, která nejenže ICT využívá jako určitý nadstandard řízení země, ale kde se ICT staly natolik důležité, že jejich správné fungování má vliv na bezpečnost celé země.

[53] Jednalo se o volby do místních zastupitelstev.

[54] K efektivitě využití ICT ve veřejné správě je také velmi zajímavým údajem čas, který je každému obyvateli šetřen skutečností, že není nutné fyzicky obíhat úřady a čekat ve frontách. Dle některých údajů se v přepočtu jedná až o 1 týden čistého času na jednoho obyvatele za rok (Luht 2014).

V lednu 2007 oznámila estonská vláda úmysl přesunout monument druhé světové války z centra Tallinnu na vojenský hřbitov nacházející se v okrajové části města. Předmětným monumentem byla bronzová socha postavy, která vyobrazovala neznámého sovětského vojáka jako osvoboditele Tallinnu, který truchlí za své padlé druhy. Tato socha byla umístěna do centra města v 50. letech po skončení druhé světové války jako připomínka jejího vítězného konce. Po revoluci v roce 1991, kdy nebyli Estonci pod přímou kontrolou Moskvy, se socha stala předmětem sporů mezi etnickými Estonci a Rusy; pro Estonce představovala symbol okupace a útlaku Sovětským svazem v období po druhé světové válce, pro Rusy naopak symbol osvobození (Healey 2013). Tento vnitropolitický rozpor se původně odehrával na pozadí blížících se parlamentních voleb, kdy bylo přesunutí sochy jednou z hlavních částí předvolební diskuze. Jednalo se o téma, na které slyšela značná část estonského obyvatelstva, a tudíž tento plán získal i značnou podporu.

Oznámení realizace přesunu sochy neuniklo ani Ruské Federaci – nejprve byla přijata Ruskou horní komorou parlamentu rezoluce odmítající přestěhování sochy, následně byl navrhnut i bojkot estonského zboží a služeb. K plánovanému odstranění se vedle politických představitelů vyjádřily i hlasy široké veřejnosti a aktivistů v Rusku, kteří přemístění sochy považovali za útok na svou národní hrdost a historii (Myers 2007a). Spor o přemístění sochy se nakonec stal artikulací sporu o identitu Estonců a náhled na druhou světovou válku a roli sovětské armády v ní (Healey 2013, Myers 2007b).

Dne 26. dubna 2007 byla bronzová socha z centra Tallinnu zakryta a připravena k přemístění. V podvečer se na místě sochy shromáždil početný zástup odpůrců přemístění[55] a v následujících hodinách započala násilná demonstrace, která trvala několik dní a která vyústila ve stovky zraněných osob a jednu oběť. Zatčeno bylo dohromady na 1300 lidí. Odhadované škody nepokojů dosáhly 4,5 milionů eur.[56]

Přemístění mělo také dohry v Moskvě, kde byli estonští velvyslanci napadeni na tiskové konferenci aktivisty skupiny Naši (Tikk a Kaska a Vihul 2010). Přemístění ostře kritizoval i prezident Putin (Healey 2013). Sergej Lavrov k této události prohlásil, že nevidí důvod, proč se lidí snaží někomu dávat vinu za historické události nebo se snaží o srovnávání komunismu s nacismem, přičemž sám tvrdil, že tato událost bude mít

[55] K první vlně protestů uvádí zdroje na 1500 protestujících (Spiegel Online 2007).
[56] Jedná se však o odhad přímých škod, nepřímé škody ve formě ušlých zisků apod. nebyly vypočítány.

závažné následky. Za relativně ostrou reakci Ruska lze považovat také pohrůžku přerušení diplomatických styků s Estonskem, když další oficiální představitelé Ruska označili přemístění za barbarské a rouhavé (Harding 2007).

Odpor k přesunutí sochy byl opravdu značný, a to ať již ze strany Ruska, tak také ze strany etnických Rusů v Estonsku. Srovná-li se však velikost estonské populace (1,3 mil.) s velikostí zde přítomného ruského etnika (cca 300 tisíc) a počtem účastníků demonstrací, je nutné říci, že aktivních demonstrací se účastnila relativně malá část z nich. Oficiální estonská vyjádření se navíc zmiňovala, že „*použité násilí ukázalo, že hlavním cílem protestujících bylo výtržnictví, ničení, porušování a rabování*“ (Spiegel Online 2007). Odpor k přemístění, který však nebyl projeven násilně při protestech, byl vlastní daleko širšímu počtu příslušníku ruské menšiny (srov. Herzog 2011).

Hlavní vlna nepokojů odezněla ráno 29. dubna, nicméně určité dohry ve fyzickém světě bylo možné zaznamenat i v pozdějších dnech.

5.1.2. Útoky

Kybernetické útoky započaly paralelně s demonstracemi proti odstranění sochy. Tikk a Kaska a Vihul (2010) rozdělují tyto útoky na dvě fáze, přičemž druhou fázi dále rozdělují na tři vlny. Každá z fází byla charakteristická a relativně odlišná – zatímco první označují za „emoční reakci“, až druhá je pro ně tím hlavním kybernetickým útokem.

První fáze útoku započala ve večerních hodinách dne 27. dubna 2007. První útok směřoval proti vládním stránkám a sítím. Později byly vedeny útoky také na online média, které reportovaly o demonstracích a celkové politické situaci a dalším subjektům soukromého sektoru.

Z veřejného sektoru lze jmenovat zejména estonské ústavní instituce, a to zejména webové stránky vlády, premiéra, prezidenta, estonského parlamentu nebo také úřadu státního dozoru. Z dalších vládních institucí pak byly napadeny i stránky jednotlivých ministerstev.[57] V neposlední řadě pak útoky směřovaly i proti webu Reformní strany, v té době vedoucí stranou vládní koalice (Tikk a Kaska a Vihul 2010). Výsledkem byla několikadenní nefunkčnost portálů a další omezení jejich dostupnosti.

[57] Zajímavým faktem je, že jediné ministerstvo, které nebylo útokem zasaženo, bylo ministerstvo kultury.

Ze soukromého sektoru se jednalo zejména o zpravodajské portály, které byly pro udržení aspoň částečné funkčnosti nuceny pod vlivem útoků často přerušovat svá připojení k Internetu tak, aby byly aspoň zčásti schopni informovat o útocích na svou zemi (Shackelford 2009).[58] Dalším značně zasáhnutým sektorem bylo bankovnictví. V určitých momentech musely být pozastaveny služby dvou největších bank kontrolující v té době 75-80 % trhu, z velké části pak musely zamezit přístupům k jejich službám ze zahraničí, což na jedné straně odstínilo velkou část škodlivých požadavků, na straně druhé to omezilo i řádné přístupy. Vzhledem k tomu, že bankovní služby jsou v Estonsku poskytovány téměř výhradně elektronicky, měly tyto útoky značný negativní vliv na společnosti a ekonomické aktivity obyvatel (Tikk a Kaska a Vihul 2010). Vedle veřejných webů bylo cíleno také na specifické servery, které byly zdrojem dat pro fungování telefonní a zejména mobilní sítě, platebních karet nebo internetové adresáře (Clarke a Knake 2010). Zasaženy byly také subjekty zajišťující sítě elektronických komunikací, se specifickým zamířením na administrátora národní domény, které mj. spravují základní internetové servery pro estonskou vládu a vzdělávací instituce. Vedle konkrétně zamířených cílů byli oběťmi i další náhodné soukromoprávní subjekty (Tikk a Kaska a Vihul 2010).

Lze vidět, že ač byly cíle velmi široké, měly svá specifická zaměření. Mobilní sítě, základní internetová infrastruktura, bankovnictví, vládní portály – z množiny možných cílů byly zasaženy právě ty, které při co nejmenší sofistikovanosti útoků mohly způsobit největší škody, resp. omezení chodu státu a jeho obyvatel. Mnoho konkrétních cílů s uvedením jejich URL a IP adres bylo poskytováno veřejně na zejména ruskojazyčných internetových fórech, což pomohlo koordinaci a efektivnosti útoků. Lze však tvrdit, že útoky nebyly vždy docela rozlišující – vzhledem k jeho šíři byly i přímo zasaženy náhodné soukromé osoby (Tikk a Kaska a Vihul 2010).

Útoky byly provedeny několika způsoby. V první fázi se jednalo zejména o jednoduché způsoby zahlcení napadaných serverů (forma DoS útoků), v pozdějších fázích získávaly jak na sofistikovanosti, tak zejména pak i na masivnosti. Jak již bylo uvedeno, hlavními

[58] Jak však poznamenává Richards (2009), zpravodajské subjekty byly do jisté míry zoufalé z toho, že vzhledem k přijatým opatřením nemohly o celé situaci kromě Estonska samotného řádně informovat zbytek světa.

typy útoků byly DDoS útoky[59] zaměřené na omezení serverů a následné poskytování služeb napadeného subjektu. Pro tyto útoky bylo velmi využíváno tzv. botnetů[60], díky čemuž se zvýšil počet zdrojů útoků. Tento typ útoků vyžaduje oproti klasickému DoS útoku menší počet aktivních subjektů k jeho provedení, jelikož umožňuje útočit i z cizích počítačů bez vědomostí jejich vlastníků.

Zajímavostí je použití webových fór pro rozšiřování informací o možnostech se k útokům připojit. Na několika takových fórech byly k nalezení informace o prioritních cílech, časech a způsobech útoků, přičemž byly dokonce vytvořeny jednoduché programy, které si každý uživatel mohl stáhnout a stát se tak vědomě součástí většího útoku (Tikk a Kaska a Vihul 2010).

Vedle disruptivních útoků bylo také použito množství defacementů[61] stejně jako vzrostl počet nevyžádaných e-mailových zpráv jak u vládních institucí, tak u soukromých subjektů.

5.1.3. Aktéři

Útoky byly vedeny na Estonsko z různých míst světa – v první fázi byly dohledány IP adresy až k ruským státním institucím, v další fázi však nemohlo být mnoho subjektů konkrétně určeno. Dohromady byly zaznamenány zdroje nacházející se ve 178 zemích (Clover 2009).

Nejviditelnějším aktérem při útocích bylo jistě hnutí Naši.[62] Mnoho členů tohoto hnutí bylo odpovědno za útoky zejména v první, emoční fázi útoku. Právě na jejich internetových fórech a stránkách byly prvotní útoky koordinovány, často se silnými emočními komentáři. Jeden z jejich představitelů, Konstantin Goloskokov, se poté vyjádřil následovně: *„Nenazval bych to kybernetickým útokem; byla to kybernetická*

[59] DoS a DDoS jsou pouze kategorie útoků s podobným efektem. Tyto útoky je možné provádět několika různými způsoby, které se liší technikou a metodologií. Ve svém důsledku se liší také náročností provedení a potřebnosti určitých technických kapacit.

[60] Botnet je sít napadených počítačů, které jsou díky jinak vloženému škodlivému kódu ovládány jiným subjektem než vlastníkem či uživatelem a je možné je tak využít i pro páchání dalších kybernetických útoků bez vědomí vlastníka (srov. Jirásek a Novák a Požár 2013).

[61] Jeden z těchto útoků například vložil na stránky estonské reformní strany „oficiální“ omluvu podepsanou premiérem Aspipem. Omluva však byla pouze v ruštině (Tikk a Kaska a Vihul 2010).

[62] Hnutí Naši je politické hnutí pro mladé Rusy. Samo je označováno jako demokratické, antifašistické, nicméně je velmi silně napojeno na vládní struktury. V době útoků na Estonsko bylo jednotným hnutím s více než 100 tisíci členy. V současné době se rozpadlo na několik odnoží.

obrana. [...] Dali jsme estonskému režimu lekci, že pokud jednají nelegálně, pak přiměřeným způsobem odpovíme" (Goloskokov 2007). Vzhledem k charakteru hnutí je však nutné považovat přinejmenším většinu útočníků jako jednotlivce jednající ve shodě.

Jak pak uvádí Tikk a Kaska a Vihul (2010), druhá fáze útoku nesla s sebou znaky daleko sofistikovanějšího útoku, které vyžadovaly takovou koordinaci a prostředky, že za nimi nemohli být pouze „obyčejní občané". Musel zde existovat další, kapacitami bohatý aktér, který byl útoku takového rozsahu schopný. Obecně se může jednat o státy nebo silné kriminální skupiny, nestátní aktéři prosazující primárně politickou agendu zpravidla takové schopnosti nemají.

Obviněn z provedení útoku byl pouze jeden student informačních technologií z Tallinnu, který přináležel k ruskému etniku.

V roce 2009 se nechal slyšet Sergej Markov, poslanec Státní dumy za Jednotné Rusko, že útoky na Estonsko byly provedeny jeho asistentem jako součást reakce občanské společnosti (Coalson 2009). Dle jeho vyjádření muselo být něco „špatného" učiněno [estonským] fašistům, přičemž je nutné čekat, že se takové reakce budou objevovat častěji. Jak však poznamenali představitelé estonského ministerstva obrany, ač posilují podezření ze zapojení Ruska do útoků, je nutné výroky Markova brát s rezervou, jelikož útoky byly provedeny natolik koordinovaně, že určitě nemohly být prací pouze jednoho či několika málo jednotlivců (Tamtéž).

5.1.4. Dopady

Nejsilnější útok byl zaznamenán 9. května, tedy v den, kdy Rusko a jeho spojenci oslavují porážku německých vojsk (The Economist 2007b). Útoky postupně slábly od 18. května, kdy byla zaznamenána poslední silná vlna DDoS útoků. Za dobu od počátku útoků bylo Estonsko postupně schopné se adaptovat některým výpadkům. Jednak se aktivizovala spolupráce vládního a soukromého bezpečnostního sektoru, jednak byla poskytnuta pomoc Estonsku ze zahraničí, zejména pak z NATO a spojeneckých zemí (Tikk a Kaska a Vihul 2010).

Proběhnuté útoky měly dopady zejména v několika oblastech a podobách. Začneme-li škodami, pak bylo zasaženo mnoho sektorů obchodu a průmyslu, které závisely na informačních a komunikačních technologiích. Nejednalo se pouze o největší hráče, ale i o menší subjekty. Útoky měly i negativní společenský efekt, když zabránily nebo

omezily komunikaci mezi, na informačních a komunikačních technologiích závislých, obyvateli Estonska (Tikk a Kaska a Vihul 2010). Útoky v některých bodech také odřízly Estonsko od zbytku světa (Richards 2009).

Co se týče mezinárodních vztahů, pak Estonsko již brzy po útocích oficiálně obvinilo Rusko z provedení útoků s poukazem na IP adresy některých moskevských státních institucí (Yasmann 2007). Rusko nařčení odmítlo a i přes silná vyjádření k přesunu sochy tvrdilo, že útoky nejsou jeho dílem. Po několika dalších výměnách Estonsko od přímých obvinění ustoupilo. Bylo však možné zaznamenat náhlou neochotu Ruska pomoct útoky zastavit a zejména pak provádět pomoc při jejich vyšetřování (Tikk a Kaska a Vihul 2010).

Odsouzen byl pouze jediný člověk. Samotná socha, kvůli které nepokoje vypukly, byla nakonec přesunuta na nepříliš vzdálený hřbitov. Estonsko se v reakci na proběhnuté útoky začalo více orientovat na problematiky kybernetické bezpečnosti a obrany.[63]

5.1.5. Analýza

Analyzovaný incident měl jeden hlavní konfliktní bod, kterým bylo odstranění bronzové sochy vojáka. Lze však tvrdit, že tato socha byla pouze zástupnickou věcí pro větší, z historie jdoucí hodnotový konflikt. Zatímco etničtí Estonci považovali období sovětské nadvlády za období útlaku, pro Rusy se jednalo o symbol národní hrdosti. Naopak, vyjádření ruských představitelů k přesunu sochy a následně poté dokonce i výzvy k rezignaci estonské vlády byly Estonskem považovány za vměšování do vnitřních záležitostí, a to i vzhledem k čerstvě proběhnutým volbám, kde bylo toto téma velmi diskutováno.

V začátku přesunu sochy Rusko emotivně deklarovalo, že citelně zasáhne. Zároveň byla značným způsobem aktivizována ruská populace, která odstranění sochy brala jako útok na svou historii a hrdost a zároveň neuznávala negativní pohled na předmětnou sochu Estonci. V rámci kyberprostoru nejprve nastoupily projevy hacktivismu, kdy samotní či srocení jedinci podnikali na základě vzájemně vyměňovaných informací kybernetické útoky s cílem potrestat Estonsko za dané události.

[63] Součástí tohoto trendu bylo zřízení Cooperative Cyber Defence Centre of Excellence při NATO. Od té doby se Estonsko stalo jednou z vedoucích zemí světa v oblasti kybernetické bezpečnosti.

Problematicky se jeví druhá fáze útoků, která byla velmi sofistikovaná a dle analýz nemohla být provedena pouhými hacktivisty. Rusko, ač ústy oficiálního představitele připustilo napojení útočníků na ruskou vládu, však vždy přímé zapojení do útoků odmítalo. Na straně druhé odmítalo na základě alibistických důvodů poskytnout Estonsku pomoc při řešení a následném vyšetřování incidentů.

Do jaké míry tato skutečnost řeší odpovědnost za provedení útoků, je diskutabilní. Jednak však odpovídá na otázku vztahu Ruska k exponovanému konfliktu, a jednak minimálně naznačuje tichý souhlas s prováděním kybernetických útoků proti jeho oponentu. Je určitě také vhodné odlišovat Rusko a ruskou veřejnost – pokud byly útoky provedeny opravdu jen nestátními aktéry bez zapojení státu, pak neochota při stíhání případných pachatelů nemůže a priori znamenat důkaz o spoluúčasti státu. Je však přinejmenším další částí mozaiky tohoto kybernetického konfliktu a zejména pomáhá odpovídat jednu z nejpodstatnějších otázek – Qui bono? V tomto ohledu lze uvažovat koncept patriotického hackingu, kdy civilisté mimo přímou kontrolu vlády se sami zapojí do útoků, jejichž cíle považují v souladu s cíli svého státu. V tomto případě ukázání síly a odporu Rusů vůči aktivitám Estonska s případným cílem donutit jej opět „zvážit“ přemístění pro ně důležitého symbolu. Rusko pak nemuselo být ochotné tyto útoky aktivně řešit, jelikož mohly být v souladu s jeho politikou (resp. aspoň s cíli této politiky) vůči Estonsku.

Rusko vedle sporu o sochu a s ním spojený náhled na historii nebylo ani nakloněno daleko silnější snaze Estonska oprostit se od jeho vlivu. Ukázka síly ruského národa prostřednictvím kyberprostoru mohla být i demonstrací svého vlivu na Estonsko a jeho nezávislost.

5.2. Litva 2008

5.2.1. Kontext

Litva je další z pobaltských zemí, která má k Ruské federaci velmi blízko. Od 18. století bylo její území více či méně součástí nebo přinejmenším pod kontrolou Ruského impéria. Podobně jako Estonsko, i Litva se stala po první světové válce nezávislým státem, který však byl oslabován neustálými (zejména teritoriálními) rozpory s Polskem a Ruskem. V rámci druhé světové války, na základě tajného dodatku Ribbentrop-Molotov byla Litva obsazena nejprve Ruskem, poté jej okupovalo Německo, aby jej v roce 1944 opět obsadil Sovětský svaz (Balkelis a Davoliute 2009). Tento stav okupace

trval de facto až do 90. let minulého století. Zejména začátek druhého období ruské nadvlády jsou poznamenány přesuny litevského obyvatelstva na Sibiř, podobně jako ostrými povstaleckými boji mezi Litevci a Rusy, později se však situace do jisté míry uklidnila na „běžnou“ úroveň okupovaných národů v sovětském prostoru. V rámci pokusu získat nezávislost v roce 1990 byly v lednu 1991 SSSR zavedeny vůči Litvě sankce, později doprovázené ozbrojeným útokem na televizní věž ve Vilniusu, při kterém bylo zabito 13 osob a více než 100 zraněných (Keller 1991a). Později v témže roce došlo k tzv. Medininkajskému incidentu, při kterém bylo zabito 6 příslušníků litevské pohraniční stráže sovětskými paramilitárními jednotkami (Keller 1991b).

Oproti Estonsku je Litva populačně jednotnější - v současné době žije v Litvě pouze 5,8 % etnických Rusů.[64] Ti se opět shlukují na několika málo místech, zejména ve Vilniusu, Klajpedě a Visaginasu.

Litva není natolik vyspělou informační společností jako Estonsko, avšak využití informačních a komunikačních technologií se pomalu zvyšuje. Tomu pomáhá litevské zaměření na tuto oblast, zejména v rámci cíle, který si Litva vytyčila – vytvořit společnost vědomostní společnost se silným důrazem na vědu, vzdělávání, kompetentní obyvatelstvo apod. do roku 2015 (Tikk a Kaska a Vihul 2010). Využívání e-governmentu je dokonce nad průměrem EU (Maskeliunas a Otas 2008). Z hlediska kybernetické bezpečnosti a ochrany je pak však Litva na relativně nízké úrovni, kdy v současnosti existuje pouze nízká míra koordinace mezi subjekty kybernetické bezpečnosti, nedostatečná spolupráce soukromého a veřejného sektoru a regulace v oblasti bezpečnosti řízení informací je nedostatečná (Sapetkaite 2012).

Bezprostřední událostí předcházející samotným útokům, které je nutné si povšimnout, je přijetí pozměňovacího návrhu k zákonu o sdružování, který upravoval svobodu slova a svobodu sdružování. Na základě tohoto zákona bylo zakázáno používat sovětské a nacistické insignie[65] na veřejných shromážděních[66] pod hrozbou vysokých pokut a dokonce i možného rozpuštění politické strany (BBC 2008).

Překvapivě, ruské etnikum v Litvě nijak závažně na tento zákon nereagovalo. Naopak Ruská federace již vzápětí po přijetí tohoto zákona projevila svou nevoli, zejména pak

[64] Největší minoritou zde zůstávají Poláci s podílem 6,6 % z celého obyvatelstva.
[65] Zejména srp a kladivo, rudou hvězdu, svastiku, stejně jako hymny obou režimů.
[66] Zajímavým faktem je, že tento zákaz neplatil pro případy, kdy se politické strany rozhodly některý z těchto znaků použít jako znak své strany (Roudik 2008).

vydáním stanovisek prezidenta a parlamentu, které tento zákon odsuzovaly s tím, že se tímto Litva pokouší „politizovat historii“ nebo také „přepsat a revidovat výsledky druhé světově války“ (Dyomkin 2008). Ruská Duma vydala také odsuzující pozici, ve které kritizovala Litvu za urážku památky sovětských vojáků, kteří bojovali ve druhé světové válce s nacisty (USA Today 2008).

Součástí této pozice byla i kritika záměru Litvy nabídnout umístění americké protiraketové obrany na svém území. Dříve v roce 2007 dokonce litevský ministr obrany Juozas Olekas prohlásil, že Litva potřebuje takový systém na svém území, aby se byla schopna ubránit případnému ohrožení ze strany nestabilních států v příštích letech (Space War 2007). Rusko tyto úvahy samozřejmě silně odmítalo a varovalo evropské státy před vybudováním zařízení protiraketové obrany na jejich území. I tyto události, ač někdy bývají v rámci analýz kybernetických útoků na Litvu přehlíženy, mohly předznamenat určitou eskalaci konfliktu a jeho projev skrze kyberprostor.

V neposlední řadě pak bývá dána jistá role i pozici Litvy při rozhovorech EU-Rusko, když právě Litva byla jedním ze států, které tyto rozhovory blokovala (Ashmore 2009b).

5.2.2. Útoky

Kybernetické útoky se objevily v době přijetí zákona o zákazu nacistických a sovětských insignií. 28. června 2008 bylo napadeno výrazné množství litevských webů, přičemž načasování útoků společně se vzrostlou aktivitou na ruskojazyčných webových fórech a diskuzích na téma zákazu používání sovětských insignií do jisté míry připomínalo útoky na Estonsko v roce 2007 (Danchev 2008a), svou závažností však estonské úrovně nedosáhlo.

Hlavními cíli útoků byly zejména webové portály různých subjektů, přičemž drtivá většina z nich byla ze soukromého sektoru. Z vládního sektoru bylo pouze 5% zasažených portálů, částečně také kvůli včasným zásahům do zabezpečení množství ostatních portálů. Všechny cíle byly hostovány stejným webhostingovým poskytovatelem přičemž většina z nich běžela na jediném serveru, jehož software nebyl řádně zajištěn a měl známou zranitelnost, které útočníci využili. Útok tak de facto směřoval proti veškerým portálům u příslušného poskytovatele bez jakéhokoli specifického zaměření (Tikk a Kaska a Vihul 2010).

Způsob útoků byl opět relativně jednotvárný, činící relativně malé škody jednotlivým subjektům. Hlavním útokem byl defacement portálů, na který útočníci umisťovali sovětské a komunistické symboly, stejně jako proti-litevské slogany, které byly vesměs ruskojazyčné (PC Tools 2008). Druhým způsobem pak bylo rozesílání e-mailového spamu na množství internetových adres, který obsahoval manifest nazvaný „Hackeři spojeni proti externím hrozbám Ruska“. Cílem tohoto manifestu bylo podněcovat obyvatelstvo k připojení se k útokům na webové portály Ukrajiny, Lotyšska a Estonska, stejně jako na západní státy jednak kvůli chování těchto států vůči ruské menšině, stejně jako kvůli podpoře rozšiřování NATO (Juhan 2008).

Oproti útoku na Estonsku byl tak tento útok daleko méně rozsáhlý a také daleko méně sofistikovaný, kdy nebyly využity pokročilé způsoby útočení.

5.2.3. Aktéři

Původci útoku nejsou do této doby známí, ač zde opět sehrály velkou roli spekulace o zapojení Ruska do jejich provedení. Litevská vláda po útocích neoznačila Rusko nebo ruské hackery za původce útoku, nicméně uvedla, že útoky byly provedeny ze zahraničí a měly zřejmě spojitost s přijetím zákazu o používání sovětských insignií (Rhodin 2008, McLaughlin 2008). Týmy rychlé reakce[67] uvedly, že útoky měly původ v teritoriích východně od Litvy (Danchev 2008a). Někteří experti se nechali slyšet, že jistá míra koordinace a plánování je pravděpodobná, jelikož jisté signály, pozvánky a agitace k útokům byly rozšířeny na internetu ještě před útoky samotnými (Rhodin 2008). Pro samostatné útoky byly pak využity servery umístěné v zemích západní Evropy (Kirk 2008).

Tikk a Kaska a Vihul (2010) pak uvádí, že dle některých zdrojů mohly být útoky přisouzeny nacionalistickým ruským hackerským skupinám, které se domlouvaly na populární ruské hackerské stránce hack-wars.ru, a které byla přisouzena jistá ústřední role při organizaci daných útoků. Danchev (2008b) pak uvádí, že zde mohly být pozorovány známky jakéhosi veřejného ospravedlňování – některé diskuze na ruských webových fórech byly vyhrocené do té míry, kdy nepřipojení se k útokům bylo považováno za znak neloajality k Rusku.[68] Snad nejlépe pak osvětluje tento, ale i jiné útoky následující prohlášení, které vydali ruští hackeři bezprostředně před útokem na

[67] V oblasti kybernetické bezpečnosti a obrany se obecně používá termín ‚Rapid Reaction Team‘.
[68] Doslova jak Danchev (2008b) uvádí: *"pokud nic neuděláte, nejste loajální ke své zemi*".

Litvu (dle Danchev [2008b]): "*Všichni hackeři této země se rozhodli se spojit, aby čelili nestydatým činům západních velmocí. Máme dost zasahování NATO na naši mateřskou půdu, máme dost ukrajinských politiků, kteří zapomněli jejich národ a myslí pouze na své zájmy. A máme také dost estonských vládních institucí, které bezostyšně přepisují historii a podporují fašismus.*[69]*"*

5.2.4. Dopady

Svým rozsahem se jednalo o relativně malý útok, určitě méně významný než na Estonsko, a to jak silou útoku, tak dopadem na společnost. Svou roli v minimalizaci dopadů také sehrála předem daná varování a vyjádření ruské hackerské komunity o odhodlanosti takové útoky nadále provádět, přičemž tyto skutečnosti poskytly Litvě jistý prostor „očekávat" podobnou aktivitu v kyberprostoru. Dopad na vládní servery byl díky tomuto relativně nízký. Naopak soukromý sektor těmito útoku utrpěl více. Útoky byly vyřešeny v relativně krátký čas, kdy k jejich vyřešení postačovala oprava zranitelností na serveru poskytovatele webhostingových služeb (Tikk a Kaska a Vihul 2010).

Několik týdnů po skončení této kampaně se odehrál další, tentokrát však izolovaný útok na litevskou daňovou správu, kdy její webový portál byl několik dnů nedostupný kvůli DDoS útoku. I v tomto případě bylo zdrojů útoků několik (Reuters 2008), nicméně některé zdroje uvádějí, že i zde bylo možné určit ruská teritoria jako místo původu útoku (Flook 2009).

5.2.5. Analýza

Tyto kybernetické útoky mohou být považovány svým rozsahem a dopadem za méně významné. Oproti útokům na Estonsko se lišily jak v době trvání, použitých technikách útoků, tak zejména v dopadech na bezpečnost a fungování země. Zajímavým aspektem je však opět kontext, ve kterém se útoky odehrály.

Ač je za bezprostřední spouštěč označováno přijetí zákona o zákazu používání sovětských insignií na veřejnosti, nelze se na tento případ dívat pouze takto úzce. Dá se říci, že přijetí zákona bylo až určitým vyvrcholením dlouhodoběji trvajícího hodnotového konfliktu, specificky pak vzhledem k pohledu na historii regionu a roli ruského etnika a ruského státu v historii Litvy. To do jisté míry potvrzují i následné útoky ve spojení s vyjádřeními ruských hackerů na svých fórech k jednotlivým činům

[69] Překlad autora této práce.

Litvy. Vyjádření představitelů ruské federace, kdy se odkazovaly zejména k nepřátelskému postoji Litvy vůči Rusku a náhledu jeho historii se slovy, že jedná o nestydatost (Dapkus 2008), pak tento sentiment v ruské společnosti potvrzovaly.

Naladění nepřátelského postoje pak zřejmě ovlivnil i záměr Litvy poskytnout své území k rozmístění systémů protiraketové obrany Spojených států, stejně jako snaha Litvy blokovat rozhovory EU-Rusko dokud nebude zajištěna větší energetická nezávislost zejména pobaltských zemí (Adomaitis 2008). Lze tak i do jisté míry uvažovat o pragmatickém a pasivním využití hodnotového konfliktu mezi Litvou a ruským obyvatelstvem k tlaku Ruské federace na Litvu z jiných, geopolitických důvodů.

Percepce Litvy, resp. lépe litevské společnosti a jejího pohledu na historii jako nepřátelského vůči Rusku, pak mohlo být pro ruskou populaci logickým závěrem, zvlášť vzhledem k velmi emočnímu popisu situace v Litvě jako fašistického režimu. Ač opět není možné jednoznačně přisoudit přímou odpovědnost za tyto útoky, je jisté, že značnou roli sehrála ruská hackerská komunita a to nejen při provádění útoků samotných, ale zejména pak v rozšiřování potřebného sentimentu mezi „relevantní" populací a následné koordinaci útoku. Zde je pak opět do jisté míry možné spatřit již uvedený koncept patriotického hackingu, kdy „uvědomělí" občané Ruska považovali za svou povinnost vyvíjet škodlivé aktivity vůči Litvě. Aktivity byly v souladu s hlavním poselstvím kritiky Litvy ze strany Ruska.

V tomto kontextu je zajímavým i vývoj v této oblasti. V polovině roku 2013 byla Litva opět obětí kybernetického útoku, který dokázal zpomalit internetovou konektivitu v zemi. Tento útok začal výhrůžným e-mailem editorům portálu DELFI[70], ve kterém neznámí aktéři požadovali odstranění článku, ve kterém obviňovali Rusko z nedovoleného kupování hlasů v soutěži Eurovision Song Contest pro ruské soutěžící. Následně DELFI utrpěl silný DDoS útok, který měl výše uvedené účinky. Útok přišel také v době, kdy Litva převzala půlroční předsednictví EU, jemuž v oblasti východní zahraniční politiky EU mělo dominovat geo-politické přetahování s Ruskem o vliv v ostatních euroasijských zemích (The Economist 2013)[71]. Další, avšak minoritní útok

[70] Jedná se o populární zpravodajský portál v baltských zemích.

[71] Do jisté míry vtipným prvkem, který však značí důležitost percepce čehokoli ruského v zahraniční pro politické představitele, byla stížnost ministra Sergeje Lavrova při rozhovoru se svým azerbajdžánským kolegou Mammadyarovem na bodování v soutěži Eurovision. Ruská soutěžící Garipova dle azerbajdžánských statistik získala více hlasů, než bylo nakonec skutečně

na tyto významné portály pak přišel v září 2014, kdy Litvu navštívil prezident USA Barack Obama. Návštěva prezidenta Obamy v Pobaltí byla v té době vnímána jako silná zpráva vůči Ruské federaci o spojenectví mezi USA a pobaltskými zeměmi (Delfi 2014).

5.3. Gruzie 2008

5.3.1. Kontext

V rámci zakavkazských zemí je Gruzie zajímavým případem vztahu mezi Ruskou federací a bývalou sovětskou republikou. Území dnešní Gruzie bylo pod nadvládou Ruského impéria od počátku 19. století. Podobně jako v dalších zemích se i zde vyskytl problém posilující rusifikace země a zároveň špatného vládnutí, které (při určité míře zjednodušení) přerostlo v ozbrojený boj proti ruské nadvládě a o snahu získat nezávislost. Gruzie vyhlásila roku 1918 samostatnost a uzavřela mírovou smlouvu s Ruskou sovětskou federativní socialistickou republikou, která však byla následně porušena a Gruzie byla následně v roce 1921 sovětským Ruskem obsazena. Podobně jako jinde v postsovětském prostoru, i Gruzie získala nezávislost až v roce 1990 (AFCEA 2012). Nelze však říci, že by od této doby byla na Rusku nezávislá; podobně jako v Pobaltí zde existovaly problémy s ruským etnikem nacházejícím se na území Gruzie. Dále se zde vyskytoval problém autonomních oblastí Gruzie, tj. zejména Jižní Osetie a Abcházie, kdy se Osetinci a Abcházové vzbouřili proti gruzínské nadvládě a za pomocí Ruska získali nad svými teritorii de facto plnou kontrolu. Ač jsou mezinárodně-právně tyto oblasti stále součástí Gruzie, jedná se de facto o samostatná území silně napojena na Rusko (AFCEA 2012).

Sledovaný kybernetický útok se odehrál na pozadí širšího konfliktu mezi Gruzií a Ruskem v roce 2008, kdy došlo k vyostření situace mezi Ruskem, Gruzií, Abcházy a Osetinci poté, co Rusko navázalo přímo styky se separatistickými vládami Abcházie a Jižní Osetie. Gruzie v čele s Michailem Saakašvilim na to reagovala posílením tlaku k zpět získání moci nad těmito oblastmi. V rámci těchto aktivit započala Gruzie rychleji budovat vojenské kapacity, které společně se Saakašviliho rétorikou vzbuzovalo na straně Jižní Osetie vážné obavy z reálné eskalace konfliktu (AFCEA 2012)[72]. Do této

soutěžící přičteno. Sám Lavrov se pak k této události vyjádřil, kdy ji označil za „pobuřující incident“ (The Moscow Times 2013). I na tyto detaily je ruská veřejnost nesmírně citlivá.

[72] Je však nutné uvést, že podobné pro-eskalační jednání měla i Ruská federace, která například před samotným konfliktem provedla masivní vojenské cvičení simulující nápadně podobné

situace také závažně zasahovalo Rusko, které se jednak snažilo o ochranu „spřízněných" menšin na gruzínském území, a jednak určitou destabilizací situace se pak pokoušelo zabránit Gruzii v postupném sbližování se západními zeměmi a zejména NATO (Tamtéž).[73]

Ač není cílem práce zaměřovat se na samostatný ozbrojený konflikt (byť velmi zajímavý), je vhodné představit aspoň základní fakta o něm - rozpory a první signály závažného konfliktu eskalovaly natolik, že 1. srpna 2008 propukly boje mezi gruzínskými vojsky a jihoosetinskými jednotkami, 7. srpna překročily gruzínské jednotky hranice Jižní Osetie a obsadily její hlavní město s odůvodněním, že pouze reagovaly na bombardování jihoosetinskými bojovníky, které porušovalo podmínky předchozího příměří. V reakci na tuto událost a na základě argumentu ochrany ruské menšiny a pozvánky Osetinců poté 8. srpna do Jižní Osetie vpadly ruské jednotky[74], které bezprostředně poté překročily i území peacekeepingového mandátu OBSE[75]. Dne 9. srpna Gruzie vyhlásila válečný stav, který trval až do 12. srpna, kdy bylo vyhlášeno příměří. V rámci tohoto krátkého konfliktu ukázaly ruské jednotky svou značnou převahu a Gruzie tak nedosáhla svých cílů (AFCEA 2012).

Vedle tohoto ozbrojeného konfliktu o oblasti Jižní Osetie a Abcházie zde však existovaly konflikty další. Příkladem může být geopolitický střet mezi Ruskem a NATO, které se přibližováním s Gruzií opět dostávalo do bezprostřední blízkosti Ruska. Za problematický bod lze považovat i vybudování vedení ropy a zemního plynu Baku – Tbilisi – Ceyhan. V návaznosti na tuto infrastrukturu přicházelo Rusko o značné množství příjmů a zároveň mu tím byla oslabována ekonomická a politická vyjednávací pozice v rámci dodávek energetických surovin Evropě (US CCU 2009).

---

události jako v srpnu 2008, stejně jako de facto připravovala své jednotky na střet s nepřítelem, gruzínskou armádou (AFCEA 2012).

[73] Přibližování Gruzie s NATO nastalo relativně brzy po zisku nezávislosti. Gruzie se aktivně snaží o přijetí za člena NATO velmi pravděpodobně z důvodu posílení své pozice a snahy mít lepší bezpečnostní pozici vůči Rusku. Gruzie bylo v roce 2008 na Bukurešťském summitu slíbeno přijetí za člena NATO a v roce 2011 byla označena za uchazečskou zemi (NATO 2011).

[74] Abcházie se následně přidala na pro-ruskou stranu, když společně s dalšími ruskými jednotkami otevřela druhou frontu útoku (Harding 2008).

[75] Peacekeepingová mise OBSE byla vytvořena v roce 1992 po gruzínsko-osetinském konfliktu. Cílem mise bylo přispět k udržení míru mezi oběma stranami. Více viz oficiální stránky http://www.osce.org/georgia-closed/44630.

Co se týče úrovně rozvoje informačních a komunikačních technologií v Gruzii, oproti pobaltským zemím je nižší, ač je její rozvoj velmi dynamický.[76] Jak však uvádí Tikk a Kaska a Vihul (2010), nízká úroveň používání internetu reflektovala i vůbec celkovou nedostatečnost informační infrastruktury země. Nutno podotknout, že v roce 2008 používala Gruzie tyto technologie pro relativně důležité služby země, tj. zpravodajství, finančnictví či vládní služby, které právě byly zasaženy nejvíce (Hollis 2011). Společně s nízkou úrovní rozvoje informační infrastruktury pak byla problémem zejména konektivita do celosvětové sítě, která byla velmi závislá na Rusku (Tikk a Kaska a Vihul 2010).[77] To z Gruzie činilo velmi dobrý cíl pro koordinovaný kybernetický útok a následnou schopnost kyberneticky tuto zemi izolovat (Tamtéž).

5.3.2. Útoky

Nejen náznaky a signály následující kybernetické kampaně, ale i samotné kybernetické útoky se objevily již v době před samotným ozbrojeným konfliktem. Několik týdnů před ruskou invazí byly DDoS útokem zasaženy stránky prezidenta Saakašviliho, které tak byly odstaveny přibližně na 24 hodin. V rámci útoků byla mezi jednotlivými daty obsažena i opakující se zpráva „win+love+in+Rusia“ (Danchev 2008c). Další předzvěst většího konfliktu přišla již v době konfliktu s Osetinci, a to 5. srpna 2008, kdy byly napadeny stránky Informační agentur OSinform[78], v jejichž důsledku byl nahrazen obsah těchto stránek obsahem webového portálu Alania TV, která je hlasem Gruzie pro obyvatele Jižní Osetie (Civil Georgia 2008). Od 7. srpna pak byla spuštěna rozsáhlá kybernetická kampaň s cílem zasáhnout informační a komunikační systémy Gruzie. Například již v pozdních hodinách tohoto dne byl ke značné části webových portálů Gruzie získán přístup nepřátelskými subjekty (Keizer 2008a).

To se projevilo zejména v den invaze ruské armády, kdy došlo k zasažení velkého množství gruzínských vládních serverů včetně portálu prezidenta, parlamentu, ministerstva zahraničí a ministerstva obrany. Zasaženy byly také stránky podporující

[76] V roce 2008, tedy v době popisovaného kybernetického útoku bylo pouze 10 % obyvatel připojeno k internetu, avšak v roce 2013 to bylo již 43,1 % obyvatel. Tento nárůst je strmější, než například u již zmiňované Litvy. Více viz UN Statistics Division (http://data.un.org/Data.aspx?d=MDG&f=seriesRowID:605).

[77] Konkrétně v roce 2008 byla Gruzie propojena přes Turecko, Arménii, Azerbajdžán a Rusko, přičemž připojení s Azerbajdžánem pak bylo z drtivé části opět propojeno do Ruska (Tikk a Kaska a Vihul 2010).

[78] OSinform informační agentura je jihoosetinskou tiskovou agenturou, která poskytuje obecné denní zpravodajství.

záměry či pozice Gruzie v paralelně probíhajícím konvenčním konfliktu (Danchev 2008d).

V rámci webových stránek prezidenta Saakašviliho došlo k zajímavému napadení 11. srpna, kdy byl do obsahu jeho stránek včleněn obrázek srovnávající Saakašviliho s Adolfem Hitlerem (Ashmore 2009b).

Specifickými cíli útoku byly také vzdělávací a finanční instituce[79] a pak zejména zpravodajské servery. Útoky byly natolik závažné, že výměna informací jak v rámci země, tak i do zahraničí byla velmi ztížena, ne-li v některých případech přímo znemožněna. Útoky tak byly schopny odstřihnout gruzínskou vládu od schopnosti informovat o probíhajícím ozbrojeném konfliktu své obyvatelstvo, a zároveň znemožnilo řádné informování zahraničních partnerů (Korns a Kastenberg 2009). Cílem útoků byla také webová fóra a související komunitní portály, které znemožnily komunikaci mezi gruzínskou IT komunitou a tím také omezila možnost obrany a případný kybernetický protiútok ze strany této části obyvatelstva (Keizer 2008b).

Několik kybernetických útoků bylo zaznamenáno také vůči ruským serverům a portálům – např. 10. srpna 2008 byly napadeny stránky RIA Novosti, které se potýkaly s několikahodinovým výpadkem (Sputnik News 2008). Byl napaden také zpravodajský server mk.ru nebo ruské bulvární stránky skandaly.ru. V neposlední řadě byl ve stejném období pod útokem i web opozičního ruského představitele Kasparova. Jak uvádí Adair (2008), tyto cíle byly napadeny stejnými útočníky, kteří se účastnili útoků na gruzínskou infrastrukturu. Možné zapojení gruzínských hackerů bylo oslabeno i s ohledem na paralyzaci gruzínské IT komunity a její neschopnosti mezi sebou komunikovat, což přinášelo nemožnost efektivní odplaty.

Způsoby útoků byly velmi různorodé. Samotné útočné techniky nebyly výrazně komplikované; skládaly se vesměs z již známých způsobů kybernetických útoků. Byly jednak využity DoS a DDoS útoky, které při existující konstelaci křehké gruzínské informační infrastruktury a nedostatečně redundantního přímého zahraničního propojení dokázaly být velmi efektivní (Ashmore 2009a). Při nich bylo široce využito botnetů, přičemž mnoho ze zdrojových útočných počítačů se nacházelo na území Turecka nebo Spojených států (Secure Works 2008). Zatímco útoky vedené skrze botnety byly více přítomny v prvních fázích útoků, v dalších fázích byly naopak více využívané útoky

[79] Zejména pak gruzínská národní banka.

prováděné jednoduchým softwarem distribuovaným širší veřejnosti prostřednictvím internetu. Vedle toho byly použity již zmíněné defacementy, kdy docházelo k umisťování proti-gruzínských vzkazů vztahujících se zejména ke srovnávání Saakašviliho se známými diktátory, resp. Gruzie jako fašistického režimu. Hollis (2011) také zdůrazňuje i špionážní aktivity a krádeže strategických dat, které v kontextu ozbrojeného útoku dávaly určitou indicii o přímém zapojení Ruska do kybernetické kampaně. I při této kybernetické kampani docházelo k triviálním útokům např. ve formě distribuce emailových adres představitelů Gruzie mezi ruskou hackerskou komunitu a následná spamovací kampaň s cílem zahltit jejich schránky, stejně jako pro případné, již sofistikované, cílené spear-phishingové[80] útoky. Masivnost a variabilitu útoků potvrzují i snahy o izolování celkové gruzínské komunikace s vnějším světem (Keizer 2008a).

5.3.3. Aktéři

Situace, kdy se kybernetické útoky odehrávaly přímo na pozadí probíhajícího ozbrojeného konfliktu, velmi nahrává úvahám spojovat odpovědnost za jejich provedení Rusku. Stejně jako v předchozích případech však není ani zde situace takto jednoduchá.

Podobně jako v případě Estonska, ani zde není přímý důkaz o provedení útoku Ruskem nebo jinými aktéry na příkaz ruského vedení (Tikk a Kaska a Vihul 2010). Někteří autoři přímé zapojení dovozují zejména z kontextu všech útoků (např. Hollis 2009), nicméně jiné zdroje jsou o mnoho opatrnější, a některé přímé ruské zapojení do celé kampaně spíše odmítají (např. US CCU 2009, Evron 2008). Ruští představitelé zapojení do kybernetických útoků důrazně odmítli, avšak opět zmínili, že je možné, že se někteří jedinci rozhodli jednat sami za sebe (Markoff 2008). Lze uvažovat, proč by při deklarované vojenské intervenci na území Gruzie zároveň Rusko nepřiznalo i své zapojení do kybernetické kampaně; důvodů může být rovnou několik od mezinárodně-právních, kdy ozbrojená intervence byla Ruskem považována za humanitární intervenci s cílem pouze zabránit Gruzii útokům na civilisty, přičemž kybernetická kampaň měla dopad daleko za tento deklarovaný cíl, po skutečné, kdy oficiální příkaz ruských představitelů ke kybernetickým útokům skutečně nemusel být dán.

[80] Phishingové útoky se snaží vyvolat důvěru u napadeného subjektu, na základě které poskytne útočníkovi citlivé údaje, popř. přímo vykoná aktivitu, kterou útočník zamýšlel. Tím může být například spuštění přiloženého škodlivého souboru, který do počítače nahraje škodlivý kód, který umožňuje útočníkovi počítač ovládat, popř. který hledá a přeposílá útočníkovi požadované data apod. Spear-phishing je typem phishingového útoku, který je cíleně zaměřen na konkrétní oběť. Často jsou při těchto útocích používány metody sociálního inženýrství pro větší šanci vzbudit u napadeného subjektu důvěru.

Shodují-li se zdroje o původcích útoků, pak zmiňují zejména ruskou hackerskou komunitu (nebo také „obyčejné“ civilisty [US CCU 2009]), nebo organizovanou kriminální skupinu Russian Business Network. Ta sehrála jednu z výrazných rolí při celé kampani (Danchev 2008d). Russian Business Network je kriminální skupina zaměřující se na kyberprostor, kde se odehrává převážná část její hlavní činnosti. Vedle hostování celé řady nelegálních služeb a portálů se také zaměřují na krádeže dat, krádeže identit nebo také provozování botnetů (např. Paganini 2013). Právě jejich botnet byl využit při hlavních útocích na gruzínské vládní sítě, je nicméně velká pravděpodobnost, že její zapojení bylo pouhou „službou“ jiné straně, kdy kromě poskytnutí infrastruktury se Russian Business Network aktivně do útoků dále nezapojovalo (Tikk a Kaska a Vihul 2010). Bylo zaznamenáno také množství útoků přímo z území Ruské federace, nicméně tyto netvořily jejich nejpodstatnější část.

Na straně Gruzie pak lze okomentovat i ostatní aktéry – paralyzace gruzínské hackerské komunity již byla rozebrána výše. Samotná vláda se snažila zejména o zisk podpory v zahraničí, která byla skutečně poskytnuta v relativně značném rozsahu. Například společnost Google poskytla doménový prostor k ochraně webových portálů ministerstva zahraničních věcí a pro gruzínské denní online zpravodajství. Jistá soukromá americká společnost v čele s etnickým Gruzíncem pak pomohla dočasně hostovat webový portál gruzínského prezidenta. Polsko pomáhalo rozšiřovat informace ze strany Gruzie dále do zahraničí skrze vydávání tiskových zpráv na svých serverech a Estonsko zase vyslalo své IT specialisty k pomoci se zvládáním útoků (Ashmore 2009a).

Kybernetické útoky trvaly ještě dlouho po skončení konvenčních operací a vyhlášení příměří mezi Ruskem a Gruzií. Jeden z posledních útoků, který se odehrál až 27. srpna 2008, byl také jedním z nejzávažnějších DDoS použitých při celé kampani. Od 28. srpna útoky postupně utichovaly.

5.3.4. Dopady

Dopady kybernetických útoků na stav, ve kterém se Gruzie nacházela, nebyl nezanedbatelný. Nejsilnějším dopadem byla zejména značně omezená možnost komunikovat a informovat své občany o probíhající situaci.[81] Tikk a Kaska a Vihul (2010) označují nedostupnost portálů ústředních vládních institucí za vážnou, s možným

[81] Závažnost řádného informování podtrhává i skutečnost, že byl v této době v Gruzii vyhlášen válečný stav.

negativním efektem na gruzínskou morálku a důvěru veřejnosti. Značný dopad měla i omezená možnost informování dění v Gruzii směrem do světa, kdy bylo velmi obtížné rozšiřovat informace a stanoviska Gruzie. V tomto ohledu pak lze pohlížet na dané útoky jako velmi sofistikovaný prostředek informační války, kdy byla Ruská federace společně s Jižní Osetií a Abcházií daleko lépe schopna říci celosvětové veřejnosti „svůj příběh“, a tím de facto převzít hlavní roli při informování o rusko-gruzínském konfliktu (Ashmore 2009a).

Nízký rozvoj ICT na jedné straně způsobil nižší dopady na každodenní život obyvatel, nicméně naopak díky související nízké kapacitě infrastruktury učinil výpadek pro esenciální služby země kritickým. Dopad na „běžný“ život veřejnosti pak měl i útok na gruzínskou centrální banku, která musela zakázat ostatním bankám používat své elektronické služby pro své klienty a další subjekty.

5.3.5. Analýza

Oproti případu Litvy je vztah mezi kybernetickými útoky a širším konfliktem daleko zřetelnější. Navíc je tento případ dobrou ukázkou situace, kdy snaha o vytvoření informační převahy nad protivníkem v rámci ozbrojeného konfliktu může ovlivnit konflikt kybernetický. Rusko se od počátku konfliktu snažilo o informační převahu a vykreslování Gruzie jako nebezpečného, zločineckého státu, a to jak mezinárodně, tak vnitrostátně. To se minimálně v rámci ruské společnosti relativně dobře dařilo. Mezinárodně byl i přes problémy s komunikací paradoxně daleko úspěšnější Saakašvili, který se vzápětí objevoval v mnohých zahraničních médiích vyjadřující utrpení bojujícího demokratického státu proti velkému ruskému kolosu (King 2008). Po několika dnech, kdy vypluly na povrch informace o výrazně protimírových aktivitách Gruzie předcházející samotné intervenci, byla značná teatrálnost Ruska při informování o konfliktu do jisté míry zbytečná (Tamtéž).

Nicméně právě popularita ruské intervence v rámci ruské společnosti může být pro analýzu kybernetického útoku v rámci tohoto konfliktu zásadní. King (2008) také uvádí, že více než 80 % Rusů souhlasilo s intervencí, přičemž více než polovina obviňovala Gruzii z vyvolání celého konfliktu a snahu Spojených států uplatňovat svůj vliv zakavkazský region za jednu z příčin celého konfliktu.

Je možné uvažovat, že samotná ruská společnost opět považovala širší konflikt za něco víc, než pouhou pomoc bratrským národům; zabránění aktivitám Gruzie mohlo být

vnímáno jako zabránění útokům na ruskou státnost a zejména pozici Ruska jako světové velmoci, která není zpochybňována, přinejmenším ve svém bezprostředním okolí.

Zaměříme-li se na ruskou, a to nikoli pouze jen hackerskou komunitu jako nejviditelnějšího aktéra provedených útok, pak US Cyber Consequences Unit[82] (2009) k tomuto uvádí: *„Kybernetické útoky proti gruzínským cílům byly provedeny civilisty s minimální nebo žádným zapojením ruské vlády nebo armády“* (US CCU 2009: 2)[83]. Zapojení obyčejných civilistů bylo vzhledem k rozšířenému sentimentu ve společnosti a zároveň rychle rozšířených informací o možnostech „přispět“ k boji velmi pravděpodobné. Korns a Kastenberg (2009: 65-66) k tomu pak dodávají: *„Naopak, internetový žurnalista vstoupil na webový portál [na kterém byla ruská hackerská komunita aktivní – pozn. autora] a stáhl si předchystaný software, který mu umožnil, pokud by se rozhodl, se připojit k útokům. Jeho stanovisko: ‚Za méně než hodinu jsem se stal internetovým vojákem. Nedostal jsem žádné telefonáty ze strany kremelských operativců ... s paranoiou, že má Kreml své ruce všude, riskujeme podcenění velkého patriotického běsnění mnoha obyčejných Rusů, kteří ... se nepochybně rozhodli jít na internet, aby se naučili, jak učinit nějakou spoušť, tak jako jsem se rozhodl já. V rámci jedné hodiny se taktéž mohli stát kybernetickými válečníky.‘“*[84]

Ač je v tomto kybernetickém konfliktu role civilistů značná, není možné se na útoky dívat pouze z pozice patriotického hackingu. Jak uvádí značná část autorů (Tikk a Kaska a Vihul 2010, US CCU 2009), koordinace, načasování a komplexnost užitých způsobů nedovoluje si jednoduše představit tyto útoky jako aktivity srocené kybernetické ruské veřejnosti. Minimálně organizátoři útoků museli mít plány ruské intervence v předstihu, přičemž zároveň byli upozornění na provádění jednotlivých pozemních operací pro načasování jednotlivých útoků (US CCU 2009). Podobně byly připraveny i seznamy stránek, na které měl být útok proveden, přičemž jeden z grafických materiálů použitých pro webové defacementy byl připraven specificky pro Gruzii již dva roky před útokem (Tamtéž). Zpráva US CCU v neposlední řadě zmiňuje i skutečnost, že žádný z útoků závažným způsobem nepoškodil žádný prvek kritické infrastruktury, které vzhledem k sofistikovanému provedení útoků a zároveň slabé

[82] Jedná se o neziskovou výzkumnou organizaci zabývající se kybernetickou bezpečností, obranou a zpravodajstvím (špionáží). Více viz oficiální webové stránky http://www.usccu.us/.
[83] Překlad autora této práce.
[84] Překlad autora této práce.

úrovni kybernetické bezpečnosti v Gruzii, musel být pravděpodobně možný. To otevírá možnost spekulacím opět o koordinaci, která však byla natolik „uvědomělá“, že k takovým akcím nedávala pokyn (Tamtéž). U pouhého kybernetického davu lze takovou uvědomělost předpokládat s menší pravděpodobností, než u specializované koordinační entity. Ač nelze aktivity jednotlivých útočníků zřejmě přičítat Rusku, je možné uzavřít, že koordinátoři útoků museli být určitým způsobem s vládnoucí nebo vojenskou částí Ruska spojeni. To může potvrzovat i časový průběh útoků vzhledem k jejich způsobům – zatímco na začátku bylo ve značné míře využito botnetů, skrze kterou bylo možné činit rozsáhlé útoky s relativně malým množstvím aktivních útočníků, v pozdějších fázích byly útoky významně ovlivněny postupnou informační kampaní s cílem povolat širší veřejnost do „kyberzbraně“. Zatímco na počátku musela existovat entita, která zařídila „objednání“ botnetové sítě u Russian Business Network a načasování útoků vůči pozemním operacím, později musela tato entita dávat instrukce širší vrstvě hackerů a dalších svolných civilistů. Některé zdroje (viz např. Leyden 2009) uvádějí, že touto entitou byla společná operace ruských FSB a GRU, nelze však vyloučit ani pouhou dobrou koordinaci v rámci ruské hackerské komunity, která byla schopna získávat informace o vojenských operacích, ve spojení s širší internetovou veřejností (Evron 2008).

Případ Gruzie je v kyberbezpečnostní komunitě zajímavým případem paralelně probíhajícího ozbrojeného a kybernetického konfliktu. Ač je souvislost mezi nimi nesporná a široká, nelze je a priori zahrnovat do stejného rámce s absolutně stejným aktérem – Ruskem jako státem a Ruskem jako národem. Bez ohledu na míru dopadů, byl vliv jednotlivých civilistů v rámci kybernetického konfliktu mnohonásobně vyšší, než v případě konfliktu ozbrojeného.

5.4. Kyrgyzstán 2009

5.4.1. Kontext

Kyrgyzstán je zemí ve Střední Asii, která jako jediná ze zkoumaných zemí přímo nesousedí s Ruskem. To ji však ani v historii a ani v dnešní době nevyjímá z vlivu, který na ni Rusko mělo, má, popř. o který usiluje, zejména pak kvůli strategické pozici jejího teritoria. Kyrgyzstán byl součástí Sovětského svazu, přičemž i zde byly sovětské zásahy do tradiční kyrgyzské kultury relativně tvrdé. V období rozpadu Sovětského svazu, kdy Kyrgyzstán usiloval o zisk nezávislosti, došlo také k několika etnickým nepokojům

mezi Kyrgyzy, Rusy a Uzbeky, následované mohutnou emigrací ze země, převážně etnických Rusů (IRIN 2006). Po zisku nezávislosti se však i tak Kyrgyzstán stal součástí Společenství nezávislých států a zejména zůstal blízkým spojencem Ruské federace (Kozlowski 2014). To se změnilo tzv. Tulipánovou revolucí, kdy byl svržen dlouho úřadující prezident Askar Akajev, přičemž nový prezident Bakijev a premiér Kulov se snažili vyvážit svou pozici vůči Rusku a spolupracovat také se Spojenými státy a dalšími zeměmi (Tamtéž). Rusko tak ztrácelo vliv na tuto zemi a opět se zde otevírala možnost vytvoření místa pro rozšiřování vojenské přítomnosti a dalšího vlivu západních zemí v bezprostřední blízkosti Ruska.

Bezprostřední kontext kybernetických útoku na Kyrgyzstán v lednu 2009 právě na tento konfliktní potenciál výrazně odkazuje. V tomto období se Kyrgyzstán rozhodoval o budoucnosti americké letecké základny v Manasu, která zde byla vybudována v rámci války proti terorismu za Bushovy administrativy a která sloužila zejména k operacím proti Talibanu na afghánském území (např. Dzyubenko 2014). Zatímco otevření této základy a následná nabídka Bakijeva v roce 2005 k možnému ponechání základny do doby, než se situace v Afghánistánu uklidní, nepřinášela výrazný odpor Ruska (Tamtéž), v roce 2009 se Rusko silně přiklonilo na stranu uzavření této základny. V případě uzavření základny pak přislíbilo Kyrgyzstánu půjčku 300 mil. dolarů a další investice zejména do energetického sektoru ve výši cca 1,7 mld. dolarů (Kozlowski 2014).

Co se rozvoje informační a komunikační infrastruktury, byla v roce 2009 situace v tomto státě relativně špatná. Na 100 obyvatel připadalo pouze 17 připojených k internetu[85]. Ve srovnání s Gruzií, kde se úroveň rozšíření informačních a komunikačních technologií mezi obyvatelstvo pohybovala kolem 10 %, se jedná o číslo větší. Lze tedy uvažovat, že i případný zásah do správného fungování kyberprostoru na území Kyrgyzstánu mohl mít jistý reálný dopad. Díky své úrovní je celá infrastruktura relativně křehká a i menší útok může ohrozit celkové fungování veřejných sítí. V neposlední řadě, dnes již v mnohých státech je řada prvků kritické informační infrastruktury závislá na moderních technologiích využívající informační a komunikační systémy a sítě. Z toho důvodu může být ohrožení byť i jen malého procenta Kyrgyzských subjektů kritické.

[85] UN Statistic Division viz poznámka č. 76.

5.4.2. Útoky

Samotné útoky započaly 18. ledna 2009 a trvaly cca 2 týdny. Útoky byly zamířeny na poskytovatele internetových služeb v zemi. Zdroje o počtu zasažených poskytovatelů se liší; například Bradbury (2009) uvádí dva, Kozlowski (2014) uvádí tři. Na první pohled se nejedná o velký rozdíl, avšak při celkovém počtu čtyř poskytovatelů může být omezení služeb jednoho poskytovatele zásadní.

Způsob útoku byl v tomto případě velmi jednolitý – jednalo se o masivní DDoS útok, který se snažil o shození serverů napadených poskytovatelů. Po celou dobu trvání byla jeho intenzita relativně dobře udržována. V návaznosti na něj bylo téměř nemožné odeslat e-mail nebo přistoupit na některé webové portály (Keizer 2009).[86] Útoky taktéž mírně narušily možnosti elektronické komunikace americké letecké základny (Tamtéž), zde však lze říci, že případný zásah nebyl natolik významný vzhledem k obyčejně se vyskytující redundanci připojení.[87] V neposlední řadě byly také zasaženy služby mobilní telefonie, která byla těmito útoky taktéž částečně omezena (Kozlowski 2014). Zajímavým bodem těchto útoků je skutečnost, že co do politického dění ovlivnily tyto útoky zejména kyrgyzskou opozici. Právě opozice využívala internet a online media pro svou agendu relativně hojně (Mamatov 2009), naopak vláda prezidenta Bakijeva na webu téměř nebyla aktivní (Keizer 2009).

5.4.3. Aktéři

O původcích útoků je opět známo pouze omezené množství informací – většina IP adres, které byly dohledány jako zdrojové adresy předmětných útoků, se nacházely na území Ruské federace. To samo o sobě není vzhledem k charakteru kyberprostoru příliš směrodatné, nicméně dokázané použití serverů dává indicie o provedení tohoto útoku podobnou skupinou ruských hackerů, jako ve výše popsaném případu Gruzie (Keizer 2009). Některé zdroje dodávají, že využití sítí lze i v tomto případě dohledat k již zmíněným kapacitám Russian Business Network (Bradbury 2009). Keizer (2009) uvádí

[86] Oproti útokům na konkrétní subjekty jsou úspěšné útoky na poskytovatele co do omezení služeb účinnější. Pokud je cílem přerušit fungování určitých technologií, služeb nebo webových portálů, pak útok na poskytovatele tím, že zahltí bod, skrze nějž se připojuje velké množství subjektů, de facto odstřihne od internetu jak subjekty poskytující tyto služby, tak i subjekty, které je mohou využívat. Tyto útoky mohou být efektivní zejména v zemích s nízkou úrovní rozvoje informační infrastruktury, kde existuje pouze omezené množství takových poskytovatelů. Lemos (2009) se nicméně domnívá, že zásah poskytovatelů byl až sekundární, přičemž prvotní útok směřoval na jiné subjekty.

[87] Některé komentáře však zasažení byť i jen části komunikačních schopnosti americké základny odmítají (viz např. Nazario 2009, sekce komentáře).

také rychlost nástupu celého útoku a hbitost jejich provedení za zvláštní znak, kdy tyto atributy značí existenci jisté předchozí přípravy k provedení útoku. Zároveň však uvádí, že oproti Gruzii nejsou v tomto případě znaky zapojení civilistů do útoků. Útoky tak byly zřejmě provedeny pouze jádrem relevantní hackerské komunity, nikoli širokým spektrem „svolných“ Rusů.

5.4.4. Dopady

V rámci dopadů je třeba uvést, že dvoutýdenní omezení internetového připojení jednotlivých kyrgyzských subjektů nepřineslo příliš značné ekonomické škody či bezpečnostní dopady, a to zejména vzhledem k rozvoji a vůbec využití informačních a komunikačních technologií v této zemi. Do jisté míry však mohly mít vliv na vnitropolitickou situaci země (Bradbury 2009).

Bakijev nakonec v únoru 2009 oznámil rozhodnutí, že požádá americkou stranu o opuštění základny. Snaha Američanů si tuto základnu udržet však prodloužila vyjednávání o jejím uzavření až do června 2009, přičemž na konci tohoto období uzavřel Kyrgyzstán s USA novou dohodu, která několikanásobně zvýšila poplatek za pronájem základny, stejně jako USA přislíbilo další investice do země.

V roce 2011 byl zvolen prezidentem Almazbek Atambajev, který měl blíže k Moskvě. Rusko následně ujistil o uzavření americké základny. K tomuto došlo v průběhu roku 2014. Rusko se neustále snažilo o upevnění svého vlivu v této zemi. Již v roce 2012 byla podepsána s ruskými představiteli nájemní smlouva, na základě které by základnu v Manasu měla (prozatím) do roku 2017 využívat ruská armáda (Dzyubenko 2014)[88].

5.4.5. Analýza

Někteří autoři relativně rychle opět dovozovali odpovědnost Ruska za tyto útoky s cílem učinit nátlak na vládu Kyrgyzstánu, aby odmítla prodloužení nájmu letecké základny Američanům a donutil je v relativně rychlém časovém rámci opustit zemi (např. Kozlowski 2014, Ashmore 2009b). Tato úvaha se může zdát i vzhledem k minulým zkušenostem s kybernetickými útoky v postsovětském prostoru relativně logická. Útoky byly provedeny s využitím sítí kriminální organizované skupiny se

[88] Podobně Rusko přistoupilo i k sousednímu Tádžikistánu, který také získal od Ruska ekonomickou pomoc výměnou za ponechání ruské vojenské přítomnosti v zemi, zejména s ohledem na případné zhoršení bezpečnostní situace po odchodu spojeneckých vojáků z Afghánistánu (Dzyubenko 2014).

stejnými znaky jako v případě Gruzie, zároveň zde existovala konfliktní oblast a motiv, proč se snažit Kyrgyzstán přitlačit; Spojené státy se nechtěly základny vzdát lehce.

Jiný pohled na tuto kybernetickou kampaň přináší Jeffrey Carr (2009b). Ten tvrdí, že kybernetické útoky neprovedlo Rusko proti kyrgyzské vládě, ale naopak, že si je objednala kyrgyzská vláda sama proti své opozici, která mj. vládu kritizovala za uvažování nad uzavřením základny, která přinášela značný ekonomický prospěch zemi. Důvodů má několik; jednak to byl efekt útoků, který neměl takový dopad na vládu nebo každodenní život obyvatel, jako na opozici vůči garnituře prezidenta Bakijeva, která prostřednictvím internetu komunikovala jak mezi sebou, tak i navenek. Druhým argumentem je pak fakt, že Bakijev již v té době byl nakloněn ruským návrhům (Carr 2009b). Některé zdroje uvádí, že už v době útoků bylo de facto rozhodnuto o uzavření základny (Jackson 2009a). V neposlední řadě se nejednalo o nijak sofistikovaný útok, který mohl být relativně jednoduše zvládnut, pokud by vyvinula kyrgyzská vláda určité úsilí (Mackey 2009). Nakonec Carr (2009b) dodává, že zkoumané útoky nápadně připomínají scénář, který se odehrál v roce 2005. Tehdy Bakijev ještě jako opoziční vůdce se snažil o nahrazení tehdejšího prezidenta Akajeva. I tehdy se udály kybernetické útoky, které efektivně blokovaly přístup k webovým portálům opozice, a znemožňovaly tak opozici efektivně komunikovat.

Tento závěr nakonec nevyvrací i následné události, kdy Bakijev v červnu 2009 prodloužil Spojeným státům smlouvu na pronájem základny a Američané tak v Kyrgyzstánu zůstali až do roku 2014. Kybernetické útoky totiž nesměřovaly proti americké základně samotné, jako právě vůči opozici.

Učinit pevný závěr však v této situaci opět nelze. Bakijev sice měl větší motivaci umlčet hlas opozice[89], nicméně podobnou motivaci mělo i Rusko samotné, které tak mohlo při využití velmi levného a nekomplikovaného nástroje skutečně ovlivnit kyrgyzskou vnitropolitickou debatu směrem k potlačení pro-amerických hlasů. Tuto pozici zaujímá Jackson (2009b), když tvrdí, že vzorec chování Ruska v kyberprostoru pro dosahování svých (geopolitických) cílů je v tomto ohledu velmi jasný.

[89] Více k politickému souboji mezi vládou a opozicí Kyrgyzstánu viz Mamatov (2009).

6. Ruská federace, kyberprostor a sousední státy

Ač není v mnoha případech možné dokázat odpovědnost za provedení útoků ruskému státu, ukázaly výše uvedené případy mezi jednotlivými státy existující konflikt, na který kybernetické útoky navazovaly. Zároveň převládá v odborné komunitě přesvědčení, že žádný z těchto kybernetických útoků nemusel být natolik závažný, popř. k nim mohlo být zabráněno již v samotném počátku, pokud by ruský stát aktivně vůči útočníkům zasáhl; co do množství kapacit a rozsahu pravomocí příslušných orgánů tyto schopnosti má. Pokud však ruský stát (přinejmenším) ponechal své obyvatele provádět kybernetické útoky vůči svým sousedním státům, je vhodné se alespoň stručně podívat na politiku Ruské federace vzhledem ke svým sousedům, která může pomoci dokreslit představený kontext jednotlivých útoků. Podobně je vhodné se pro lepší zachycení kontextu podívat i na postoj Ruska ke kyberprostoru jako celosvětové doméně.

6.1. Politika Ruské federace k sousedním zemím

Pojmout současnou ruskou zahraniční bezpečnostní politiku ve všech důležitých souvislostech na několika málo odstavcích je vzhledem k šíři této problematiky a dynamickému vývoji v této oblasti téměř nemožné. Práce se zde proto pokusí spíš o nastínění některých jejích aspektů, které pomohou lépe dokreslit celkový kontext představených útoků.

Rusko se od rozpadu Sovětského svazu nikdy nevzdalo aspirace na světovou velmoc podobné váhy, jako jsou Spojené státy. Strategie národní bezpečnosti Ruské federace do roku 2020, která byla přijata výnosem prezidenta v květnu 2009, v mnoha oblastech specifikovala postoj Ruska ve vztahu k jeho zájmům, přičemž jedním z nich je i obnovení své mezinárodní pozice.[90]

S tím souvisí i zajištění svého nejbližšího okolí, zejména pak zajištění vlivu na relevantní země, kde pozice západních zemí posilují. V tomto ohledu se pak aktivně snaží o zabránění rozšiřování vlivu NATO a EU do těchto zemí (Stewart 2014), případně rovnou jejich přistoupení k těmto organizacím. Na jedné straně je také možné spatřit snahu o užší ekonomickou spolupráci se sousedními státy a snahu sousední,

[90] Vzhledem k relativně nedávným událostem v souvislosti s konfliktem na Ukrajině již není pro zjištění některých pozic Ruska v mnoha ohledech použitelná, aspirace na světovou velmoc je však stále patrná.

zejména eurasijské a asijské, země inspirovat k hlubší spolupráci s Ruskem (Monaghan 2010), na straně druhé vůči nim přistupuje s jistou tvrdostí a nevyhýbá se ani zásahům do vnitropolitických záležitostí.

Vedle snahy o zabezpečení situace u sousedních států s cílem zabránit rozšiřování konfliktů a destabilizace příhraničních oblastí, je značným argumentem pro zasahování do záležitostí sousedních zemí i cíl Ruska chránit ruské občany v zahraničí. Rusko nejenže má tento cíl stanoven v již zmíněné národní bezpečnostní strategii, ale odkazuje se k němu při mnohých konfliktech se sousedními státy, kdy v případech užití silových metod hovoří o humanitární intervenci[91] (např. Wild 2008). Tato ochrana však nemíří pouze vůči fyzické ochraně jednotlivých občanů, ale také pojímá jejich práva a zejména pak jejich zájmy (např. Putin 2014). Co vše pak lze zahrnout mezi takové zájmy? Je možné pod ně zahrnout i výpad vůči v Rusku obecně přijímanému výkladu dějin? Nebo se může jednat o zájem ruských občanů žijících v blízkém zahraničí být pod větší „ochranou“ Ruské federace? Vzhledem k uvedeným případům je interpretace těchto zájmů široká a otevřena různým výkladům v souladu s pragmatickou zahraniční bezpečností politikou Ruska.

Ochrana ruských občanů v zahraničí tak opět pravděpodobně souvisí s cílem posílit svůj vliv na dění v sousedních zemích, kde se zpravidla nacházejí početné ruské menšiny. Ruská federace má takto prostor pro budování své sféry vlivu a ovlivňování situace u svých sousedů dle aktuálních zájmů (srov. STRATFOR 2009).

Na v této práci uvedené kybernetické konflikty je tak možné se dívat i z této pozice, kdy jejich projevy mohly být v souladu s politikou Ruska tím, že vedle zamýšlených manifestních efektů ukazovaly sekundárně i vliv, který Rusko na zasažené země dokáže mít, bez toho aniž by došlo k uplatnění jakékoli odpovědnosti za jejich provedení. Stejně tak mohly v některých případech ukázat jednotu a sílu ruské veřejnosti (tedy nejen pouze ruského státu ve smyslu vládních či vojenských struktur) i v kyberprostoru, zejména při útocích na Litvu a Gruzii.

[91] Argument ochrany ruských občanů v zahraničí byl jedním z nosných právě při intervenci Ruska v Gruzii v roce 2008. Viz např. oficiální vyjádření prezidenta Medveděva dostupné ke dni 18. 5. 2015 na http://archive.kremlin.ru/eng/speeches/2008/08/08/1553_type82912type82913_205032.shtml

6.2. Rusko a kyberprostor jako doména pro prosazování zájmů

Rusko přistupuje ke kyberprostoru a souvisejícím aspektům relativně odlišně od většiny západních zemí. Ve svých vlastních pozicích často neužívá pojmy s přídomkem „kyber"; naopak více kyberprostor popisuje ve světle informační politiky (Thomas 2009).[92] Hlavním zájmem Ruska v oblasti kybernetické bezpečnosti tak není ani tak zajistit funkčnost informačních a komunikačních systémů a sítí pro informační svobody jednotlivců, jako spíše zajistit jistý řád a pořádek přímo v rámci informací, které mohou být kyberprostorem přenášeny. Tyto snahy se projevují různými způsoby, od budování státních kybernetických kapacit, po snahu hlouběji kontrolovat kyberprostor a regulovat tak chování obyvatel v něm[93].

Charakteru kyberprostoru nejen jako prostředí, ve kterém se nacházejí hrozby pro bezpečnost Ruska, ale také i jako příležitostí, které poskytuje, si je Rusko relativně dobře vědomo. I proto byly na oficiální úrovni přijaty strategické dokumenty věnující se kyberprostoru, resp. informačnímu prostoru a přístupu Ruska k němu. První z těchto je obecná Doktrína informační bezpečnosti z roku 2000, druhou je pak relativně nedávný dokument s názvem Koncepční náhledy na činnosti ozbrojených sil Ruské Federace v informačním prostoru z roku 2012. Zejména druhý dokument zmiňuje i cíl Ruska být schopno prostřednictvím kyberprostoru aktivně zabránit eskalaci nebo zamrznutí konfliktu a jeho vstup do takové fáze, která by materiálně zvýšila cenu za vyřešení takového konfliktu (CCDCOE 2012: 11). Koncepce obsahuje i další ustanovení podobného rázu, které podtrhují snahu o dosažení schopností činit rozhodující aktivity v případě kybernetického, resp. informačního konfliktu.

Rusko nijak nepopírá existenci svých schopností a zejména ambice být důležitou silou i v rámci kyberprostoru, který tak pojímá jako další z domén, ve kterých lze a je nutno své zájmy prosazovat. Zároveň svým přístupem ke kyberprostoru se staví mezi země

[92] Rusko je jednou ze zemí, která se v rámci Mezinárodní Telekomunikační Unie při OSN drží používání pojmu informační bezpečnost místo kybernetická bezpečnost. Tento rozdíl není pouhou nuancí – odkazuje spíše k chápání kyberprostoru Ruskem jako prostředí informační politiky; zatímco kybernetická bezpečnosti je obsahově neutrálním pojmem odkazujícím k zabezpečení fungování počítačů a sítí a dostupnosti, integrity a důvěrnosti dat, informační bezpečnost zahrnuje i regulaci informací, které se v kyberprostoru uchovávají, zpracovávají a vyměňují.

[93] Příkladem za všechny pak mohou být snahy o regulaci vedení internetových blogů. Současné době je každý jedinec, který má blog, jehož návštěvnost je vyšší než 3000 přístupů denně, povinen jej zaregistrovat jako „mediální prostor" u příslušného úřadu (Milashina 2014). Tato regulace jde nad rámec běžné regulace vyskytující se v západních státech.

snažící se o kontrolu nad touto doménou, kdy nesouhlasí se současným decentralizovaným konceptem jeho řízení.

Pokud však docházíme k závěru, že v Rusku existují jednak normy a vůbec politická vůle regulovat hlouběji chování jedinců v kyberprostoru i ve smyslu informací, které jsou vyměňovány, a zároveň má Rusko samotné kapacity prosazovat v kyberprostoru své zájmy, stejně jako má represivní kapacity mnohé jedince porušující dané normy dopátrat, nabízí se otázka – pokud Rusko není za samotné výše uvedené útoky odpovědné, proč učinilo pouze minimum kroků k tomu, aby útoky přestaly nebo jim bylo zabráněno? I pokud by nebyly škodlivé aktivity vycházející z území Ruska trestné podle ruských zákonů, pak přinejmenším způsobovaly porušení norem mezinárodního práva v rámci ‚due dilligence'. Opět – není zde cílem dokázat odpovědnost za provedení daných útoků. Cílem je poukázat na kontext a možný motiv činnosti či nečinnosti Ruska v rámci uvedených kybernetických útoků. Autor této práce se domnívá, že Rusko vždy mohlo přinejmenším přispět ke zmírnění, ne-li zastavení uvedených útoků – jaká pak byla motivace zde nechat volnou ruku (jak uvedl Sergej Markov v případě Estonska) občanské společnosti k projevům svého rozhořčení a provádění těchto útoků? Poukazuje-li výše uvedené na jednu věc, pak je to přinejmenším potenciální pragmatické využívání kybernetických střetů v postsovětském prostoru z hlediska cílů a zájmů, které ruská zahraniční politika má, a to bez ohledu na skutečnost, zdali bylo Rusko přímo či nepřímo za dané útoky odpovědné, či nikoli (srov. Jackson 2009b, Carr 2015).

7. Závěr

Využívání kybernetického prostředí v rámci konfliktů pro prosazování svých zájmů není novodobou záležitostí. Výzkum kybernetických konfliktů jako jisté podmnožiny obecného výzkumu konfliktu má i svou historii, nicméně mnoho pojmů a konceptů z této oblasti je však stále neustálených. Proto se práce dříve, než přistoupila k jednotlivým událostem, zaměřila na vymezení jednotlivých pojmů, stejně jako se na vhodných místech pokusila o poukázání na zvláštnosti a dopady různých existujících definic. Je-li vhodné zde něco zdůraznit, pak zejména to, že kyberprostor je sice doména založena na svobodném jednání aktérů v něm, avšak není zcela nezávislá. Státy mohou ovlivňovat jak bezpečnost kyberprostoru, tak i chování jednotlivců v něm. Jednání uživatelů není nekontrolovatelné, a odvíjí se i od existujících právních, politických a dalších opatření. To má dopad i na přístup států ke kyberprostoru jako doméně, ať již jako společenské, ekonomické, politické nebo vojenské.

Z tohoto hlediska pak práce přistoupila k diskuzi nad specifiky, které má výzkum kybernetických konfliktů. Konkrétně se zaměřila na vlastnosti kyberprostoru a jeho dopad na hlavní konfliktní atributy, tj. aktéry, oblast střetu, napětí a jednání.

Na tomto základě pak přikročila k deskriptivní analýze jednotlivých kybernetických útoků na Estonsko v roce 2007, Litvu a Gruzii v roce 2008 a Kyrgyzstán v roce 2009. V rámci těchto případů pak představila jejich kontext, popsala samotné útoky se zaměřením na jejich cíle a způsoby, načež přistoupila k popisu možných aktérů a zdrojů útoků. Následně se pak práce pokusila diskutovat vztah představených skutečností a kontextu útoků ve vztahu k existujícím konfliktům, které souvisely nebo mohly s předmětnými útoky souviset.

Ve všech sledovaných případech bylo možné spatřit, že se útoky skutečně odehrály na pozadí širšího, v té době eskalovaného konfliktu. V Estonsku se jednalo o přemístění bronzové sochy neznámého sovětského vojáka, která byla symbolem o nahlížení na roli ruského národa v estonské historii. V Litvě byl naopak v době útoků přijat zákon o zákazu používání sovětských insignií, který opět popudil zejména Ruské představitele s ohledem na argument, že se Litevci snaží o přepisování historie. Nejviditelnější konflikt odehrávající se na pozadí kybernetických útoků bylo možné spatřit v případě Gruzie, kde kybernetická kampaň byla synchronizována s intervencí ruských jednotek v Jižní Osetii. V případě Kyrgyzstánu byla naopak situace o mnoho méně jasná, když

mohl být kybernetický útok proveden z vícero důvodů, resp. na základě různých motivací.

Z velké části bylo možné spatřit silné zapojování jednotlivců (zejména, ale nikoli pouze jen ruských civilistů) do probíhajících útoků. Patriotický hacking tak, jak byl popsán v teoretické části práce, bylo možné vidět zejména na případě Gruzie, pak také Estonska a Litvy. S tímto souvisí i viditelná schopnost ruské společnosti vytvářet potřebný sentiment, který vytvářel a prohluboval konfliktní potenciál mezi Rusy a zasaženým státem.

Spojujícím prvkem byl i přítomný boj o vliv na politiku zasažených zemí. Ač se vesměs nejednalo o akutní události, jak jsou uvedeny výše, ve všech zemích bylo možné spatřit střet vlivu Ruska a aktivit západních zemí v zasažených státech. V tomto ohledu je možné vidět i jistý pragmatický přístup Ruské federace, kdy je možné uvažovat, že kybernetické útoky skutečně z velké části ponechávala na ruské veřejnosti (a hackerské komunitě), čímž jednak mohla dosáhnout na jedné straně demonstrace svého vlivu na zasažené země, na straně druhé však nemohla být účinně odpovědna za jejich provedení.

Konfliktní reakce skrze kyberprostor má velmi efektivní poměr mezi jednoduchostí provedení takové akce, značnou viditelností, a zároveň malou rizikovostí pro útočníka. Rozhořčení v ruském denním tisku by nemělo pro cílové (pobaltské) země svou váhu. Diplomatická řešení jsou pak často dvojsečná vzhledem k jejich možné reciprocitě. Závažnější vojenská řešení by pak byly naprosto nepřiměřené. Kybernetické útoky mají výborný potenciál, jak relativně jednoduše a efektivně vyjádřit neslučitelnost aktivit jednoho aktéra se zájmy či hodnotami aktéra druhého.

„Lidé, kteří byli v KGB nebo v jiné části vlády, a kteří se nyní pohybují v oblasti počítačové bezpečnosti, již v minulosti říkali ‚Budeme se spoléhat na těchto schopnostech, protože v tom pro nás není žádný risk' řekl Jackson. ‚Používání kybernetických milicí chrání ruskou vládu před případnou vinou'" (Kaizer 2009)[94].

Ač je tedy možné uvažovat sílu zapojení ruských civilistů do útoků a případnou ruskou toleranci jejích aktivit, popsané případy také ukázaly, že ne veškeré aktivity spojené

[94] K tomuto pak lze dodat, že se ani nemusí jednat o milice dle běžných definic (např. Mareš 2012), jako spíše o ad hoc ‚kybersrocené' civilisty, u kterých je podporován ‚správný' sentiment.

s útokem byly provedeny pouze jimi. Přinejmenším v případě Gruzie (a pravděpodobně i Kyrgyzstánu) byla dokázána role kriminální skupiny Russian Business Network. Zároveň vzhledem ke koordinaci a načasování útoků, stejně jako vzhledem k sofistikovanosti jejich provedení (Estonsko a Gruzie) pak mnoho autorů vyvozuje, že je zde nutné uvažovat i aktéra dalšího, který by tyto potřebné schopnosti měl. Někteří autoři přímo odkazují k ruské vládě, jiní za tím vidí operace zpravodajských služeb, jiní spekulují o síle určité organizace složené z vícero kruhů. Dokázat propojení jednotlivých aktérů a orchestraci kybernetických útoků ze strany ruských státních struktur je téměř nemožné. Nedávné události na Ukrajině však vrhají na přístup Ruska k využívání „nepřiznaných" kybernetických útoků jiné světlo.

Když došlo v roce 2014 na Ukrajině k občanským nepokojům, které byly následovány ruskou intervencí na Krym a jeho připojení k Rusku společně s eskalací konfliktu na východě Ukrajiny mezi ukrajinskými složkami na jedné straně a proruskými separatisty a (téměř jistě) Ruskem na straně druhé, vyskytly se i zde kybernetické útoky zaměřené zejména proti ukrajinským vládním serverům, kritické infrastruktuře, mobilním službám, stejně jako např. serverům sčítajícím volební data (např. Limnell 2014).

Ač není prostor tento konflikt na tomto místě hlouběji analyzovat, dle mnoha informací z nich vyplývá několik závěrů. Jednak se útoku opět účastnila řada civilních subjektů, která byla podporována náladou v ruské společnosti (Boulet 2015); v rámci kontextu se také útoky vyskytly v momentě aktuální politické krize, která však měla hlubší kořeny (např. Chalupa 2013). V neposlední řadě Rusko opět odmítlo odpovědnost za provedení těchto útoků (např. Bender 2014).

Zejména k poslednímu bodu však existence mnoha důkazů o zapojení ruských ozbrojených sil do bojů na východě Ukrajiny, i přes neustálé popírání této účasti, vzbuzuje relativně oprávněné obavy o existenci podobné strategie i v kyberprostoru. I pokud Rusko nebylo odpovědné za spáchání útoků popsaných v této práci, poznatky z ukrajinského konfliktu mohou měnit náhled na roli Ruska v rámci kybernetických konfliktů. Nakonec je tak Healeyho přístup (2013), který nabádá ke spojování kampaní kybernetických útoků s relevantní geopolitickou situací, lépe podložený pro přístup ke kybernetickým konfliktům v postsovětském prostoru. Případ Kyrgyzstánu na straně druhé ukázal i nejistotu, se kterou se zde musí výzkum kybernetických konfliktů potýkat, a to zejména vzhledem k pluralitě aktérů a jejich konfliktů.

Dle výše uvedeného odpověděla tato práce na položené výzkumné otázky a snad přispěla k osvětlení průběhů, kontextů a možných motivací uvedených kybernetických konfliktů v postsovětském prostoru. Slabinou této práce je šíře tématu, která neposkytovala možnost zaměřit se na vícero jednotlivých detailů předmětných útoků. Na straně druhé by poté bylo obtížnější ukázat podobnosti a rozdílnosti mezi vybranými konflikty. Práce pak také jistě mohla detailněji představit existující souvislosti, které se k daným kybernetickým útokům váží. Do budoucna může být zajímavé se zaměřit na povahu pravděpodobných útočníků zejména z řad veřejnosti a na jejich postoje vůči politice Ruska, stejně jako na schopnost Ruska nebo ruské společnosti budovat správný sentiment potřebný pro aktivizaci relevantní části veřejnosti.

8. Příloha č. 1 - slovník

DoS / DDoS útok

Technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem z mnoha vektorů (Vláda ČR 2014: 24).

botnet

Sítě infikovaných počítačů zneužitelných k páchání kriminálních aktivit, které díky přístupu k výpočetnímu výkonu mnoha tisíců strojů současně mohou provádět nezákonnou činnost ve velkém měřítku – zejména útoky DDoS a distribuci spamu (Vláda ČR 2014: 24).

defacement

Průnik do webového serveru protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. Zkreslení není skrytí, naopak, usiluje o medializaci a jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka (Jirásek a Novák a Požár 2013: 31).

phishing

Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele (Jirásek a Novák a Požár 2013: 71).

spear-phishing

Sofistikovanější útok typu *phishing*, který využívá předem získané informace o oběti. Díky většímu zacílení na konkrétní uživatele dosahuje tato metoda většího účinku než běžný útok typu *phishing* (Jirásek a Novák a Požár 2013: 97).

9. Zdroje

1. **Adair, Steven**. 2008.: „Georgian Websites Under Attack - DDoS and Defacement“. Shadowserver.org. Cit. dne 18. 5. 2015. Dostupné z: http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811

2. **Adomaitis, Nerijus**. 2008.: „Lithuania Ready to Block EU's Russia Talks“. The Moscow Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.themoscowtimes.com/sitemap/free/2008/4/article/lithuania-ready-to-block-eus-russia-talks/362346.html

3. **AFCEA**. 2012.: The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict. Cit. dne 18. 5. 2015. Dostupné z: http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf

4. **Applegate, Scott D**. 2009.: Cyber Warfare - Addressing New Threats in the Information Age. Cit. dne 18. 5. 2015. Dostupné z: https://gmu.academia.edu/ScottApplegate/Papers

5. **Arquilla, John.** 2013.: „Twenty Years of Cyberwar“ In: Journal of Military Ethics. roč. 12, č. 1, s. 80-87.

6. **Arquilla, John a Ronfeltd, David**. 1997.: Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND. 525 s.

7. **Ashmore, William C**. 2009a: Impact of Alleged Russian Cyber Attacks. Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College. Cit. dne 18. 5. 2015. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf

8. **Ashmore, William C**. 2009b.: Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review, č. 11, s. 4-40.

9. **Balkelis, Tomas a Davoliute, Violeta**. 2009.: National Report on Lithuania. How the Memory of Crimes Committed by Totalitarian and/or Other Repressive Regimes in Europe is Dealt With in the Member States. Cit. dne 18. 5. 2015. Dostupné z: https://www.academia.edu/10066635/National_Report_on_Lithuania._How_the_

Memory_of_Crimes_Committed_by_Totalitarian_and_or_Other_Repressive_Regimes_in_Europe_is_Dealt_With_in_the_Member_States

10. **Bannon, Ian a Collier, Paul**. 2003: Natural Resources and Violent Conflict. Washington, D.C.: The World Bank, xviii, 409 s. ISBN 0821355031.
11. **Barlow, John P**. 1996.: „A Declaration of the Independence of Cyberspace“ In: Postcards from the Net:An Intrepid Guide to the Wired World (eds. J. Casimir ed.), s. 365–7. Sydney: Allen and Unwin.
12. **Bartos, Otomar J**. **a Wehr, Paul**. 2002.: Using Conflict Theory. New York: Cambridge University Press. xi, 219s.
13. **Bastl, Martin**. 2007.: Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví. Dizertační práce. Brno: Masarykova univerzita.
14. **BBC.** 2002.: Estonia removes SS monument. Cit. dne 18. 5. 2015. Dostupné z: http://news.bbc.co.uk/2/hi/europe/2148732.stm
15. **BBC**. 2003.: US hackers told to leave Iraq alone. Cit. dne 18. 5. 2015. Dostupné z: http://news.bbc.co.uk/2/hi/technology/2760899.stm
16. **BBC**. 2005.: Russia denies Baltic 'occupation'. Cit. dne 18. 5. 2015. Dostupné z: http://news.bbc.co.uk/2/hi/europe/4517683.stm
17. **BBC**. 2008.: Lithuanian ban on Soviet symbols. Cit. dne 18. 5. 2015. Dostupné z: http://news.bbc.co.uk/2/hi/europe/7459976.stm
18. **Bender, Jeremy.** 2014.: EXPERT: "The Ukraine-Russia Cyberwar Is 'More Serious And Damaging' Than The Annexation Of Crimea". Business Insider online. Cit. dne 18. 5. 2015. Dostupné z: http://www.businessinsider.com/ukraine-russia-cyberwar-extremely-serious-2014-3
19. **Boulet, Gertjan**. 2015.: "Cyber Operations by Private Actors in the Ukraine-Russia Conflict: From Cyber War to Cyber Security" In: Amercian Society of International Law online. Cit. dne 18. 5. 2015. Dostupné z: http://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber
20. **Bradbury, Danny**. 2009.: „The fog of cyberwar“. The Guardian online. Cit. dne 18. 5. 2015. Dostupné z:

http://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access

21. **Carr, Jeffrey**. 2009a.: Inside Cyber Warfare: Mapping the Cyber Underworld. Sebastopol: O'Reilly Media. 240s. ISBN 1449382991.

22. **Carr, Jeffrey**. 2009b. In Mackey, Robert. 2009.: „Are 'Cyber-Militias' Attacking Kyrgyzstan?" The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?_r=0

23. **Carr, Jeffrey**. In: Springer, Paul J. 2015.: Cyber Warfare: A Reference Handbook. Santa Barbara, CA: ABC-CLIO. 340 s. ISBN: 1610694449

24. **CCDCOE**. 2012.: Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. Neoficiální překlad. Cit. dne 18. 5. 2015. Dostupné z: https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

25. **Clarke, Richard A a Knake, Robert K**. 2010.: Cyber war: the next threat to national security and what to do about it. New York: Ecco. s. 290. ISBN 9780061962233.

26. **Chalupa, Andrea**. 2013.: "How to Explain What's Happening in Ukraine". Time online. Cit. dne 18. 5. 2015. Dostupné z: http://ideas.time.com/2013/12/17/how-to-explain-whats-happening-in-the-ukraine/

27. **Choucri, Nazli a Goldsmith, Daniel**. 2012.: „Lost in cyberspace: Harnessing the Internet, international relations, and global security" In: Bulletin of the Atomic Scientists, roč. 68, č. 2, s. 70-77.

28. **Civil Georgia**. 2008.: S.Ossetian News Sites Hacked. Cit. dne 18. 5. 2015. Dostupné z: http://www.civil.ge/eng/article.php?id=18896

29. **Clover, Charles.** 2009. „Kremlin-backed group behind Estonia cyber blitz". Financial Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz3aWCUmtAu

30. **CNSS – Committee on National Security Systems**. 2010. National Information (IA) Glossary. Instrukce CNSS č. 4009 ze dne 26. dubna 2010. Cit. dne 18. 5.

2015. Dostupné z:
http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

31. **Coalson, Robert.** 2009.: „Behind The Estonia Cyberattacks“. Radio Free Europe online. Cit. dne 18. 5. 2015. Dostupné z:
http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html

32. **Danchev, Dancho**. 2008a.: „300 Lithuanian sites hacked by Russian hackers“. ZDNet. Cit. dne 18. 5. 2015. Dostupné z: http://www.zdnet.com/article/300-lithuanian-sites-hacked-by-russian-hackers/

33. **Danchev, Dancho**. 2008b.: Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced. Cit. dne 18. 5. 2015. Dostupné z:
http://webcache.googleusercontent.com/search?q=cache:jgfyjmzwHtAJ:www.circleid.com/posts/87870_lithuania_internet_attack_russian_hacktivists/+&cd=1&hl=cs&ct=clnk&gl=cz

34. **Danchev, Dancho**. 2008c.: Georgia President's web site under DDoS attack from Russian hackers. Cit. dne 18. 5. 2015. Dostupné z:
http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/

35. **Danchev, Dancho**. 2008d.: Coordinated Russia vs Georgia cyber attack in progress. Cit. dne 18. 5. 2015. Dostupné z:
http://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

36. **Dapkus, Liudas**. 2008.: „Lithuanian lawmakers ban display of Soviet symbols“. USA Today online. Cit. dne 18. 5. 2015. Dostupné z:
http://usatoday30.usatoday.com/news/world/2008-06-18-1006014433_x.htm

37. **Deeks, Ashley**. 2013.: „The Geohraphy of Cyber Conflict: Through a Glass Darkly“ In: International Law Studies, roč. 89, p. 1; Virginia Public Law and Legal Theory Research Paper No. 2013-10.

38. **Delfi**. 2014.: DELFI subjected to cyber attacks. Cit. dne 18. 5. 2015. Dostupné z:
http://en.delfi.lt/lithuania/society/delfi-subjected-to-cyber-attacks.d?id=65734904

39. **Denning, Dorothy E. R**. 1999.: Information Warfare and Security. Reading: Addison-Wesley. 522 s. ISBN 0201433036.

40. **Denning, Dorothy E. R**. 2001.: „Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy“ In: Networks and Netwars: The Future of Terror, Crime, and Militancy (J. Arquilla and D. F. Ronfeldt eds.), s. 239-288.

41. **Diehl, Paul a Goertz, Gary**. 2000.: War and Peace in International Rivalry. Ann Arbor, MI: University of Michigan Press. Cit. dne 18. 5. 2015. Dostupné z: https://www.press.umich.edu/pdf/0472111272.pdf

42. **Dipert, Randall R**. 2013.: „Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy“ In: Journal of Military Ethics, roč. 12, č. 1, s. 34-53

43. **Drmola, Jakub**. 2014.: „Looking for Insurgency in Cyberspace“ In: Central European Journal of International and Security Studies (CEJISS), Prague: Metropolitan University Prague, 2014, roč. 8, č. 4, s. 22-44. ISSN 1802-548X

44. **Dyomkin, Denis**. 2008.: „Russia condemns rewriting of World War Two history“. Reuters. Cit. dne 18. 5. 2015. Dostupné z: http://uk.reuters.com/article/2008/06/23/uk-belarus-russia-history-idUKL221014120080623

45. **Dzyubenko, Olga**. 2014.: „‘Mission accomplished‘ for U.S. air base in pro-Moscow Kyrgyzstan“. Reuters. Cit. dne 18. 5. 2015. Dostupné z: http://www.reuters.com/article/2014/03/06/us-kyrgyzstan-usa-base-idUSBREA251SA20140306

46. **Elliot, Steven a Payton, Theresa**. 2010.: Cyber Warfare and the Conflict in Iraq. Cit. dne 18. 5. 2015. Dostupné z: http://www.infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html

47. **Elsuwege, Peter van**. 2004.: Russian-speaking minorities in Estonia and Latvia: problems of integration at the threshold of the European Union. Pracovní dokument č. 20. Flensburg: European Centre for Minority Issues (Ed.). ISSN 1435-9812

48. **Euractiv**. 2007.: Estonia first country in the world to introduce internet voting. Cit. dne 18. 5. 2015. Dostupné z: http://www.euractiv.com/egovernment/estonia-country-world-introduce-news-214896

49. **Evron, Gadi**. 2008.: Georgia Cyber Attacks From Russian Government? Not So Fast. Cit. dne 18. 5. 2015. Dostupné z: http://www.csoonline.com/article/2123048/emergency-preparedness/georgia-cyber-attacks-from-russian-government--not-so-fast.html

50. **Federální ministerstvo vnitra Spolkové republiky Německa**. 2011.: Strategie kybernetické bezpečnosti pro Německo. Cit. dne 18. 5. 2015. Dostupné z: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=5B6636607CB58EFBB61431566F7E5B15.2_cid334?__blob=publicationFile

51. **Flook, Kara**. 2009.: Russia and the Cyber Threat. Cit. dne 18. 5. 2015. Dostupné z: http://www.criticalthreats.org/russia/russia-and-cyber-threat

52. **Gartzke, Erik**. 2013. „The myth of cyberwar: Bringing war on the internet back down to earth“ In: International Security, roč. 38, č. 2., s. 41-73.

53. **Geers, Kenneth**. 2013. In: Kerner, Sean M. 2013.: Has World War C (Cyber) Already Started? Cit. dne 18. 5. 2015. Dostupné z: http://www.eweek.com/security/has-world-war-c-cyber-already-started.html

54. **Goloskokov, Konstantin**. 2009. In: Clover, Charles. 2009. „Kremlin-backed group behind Estonia cyber blitz“. Financial Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz3aWCUmtAu

55. **Hakken, David**. 1999.: Cyborgs @ Cyberspace? An Ethnographer Looks to the Future. New York: Routledge.

56. **Harding, Luke**. 2007.: „Russia up in arms after Estonians remove statue of Soviet soldier.“ The Guardian online. Cit. dne 18. 5. 2015. Dostupné z: http://www.theguardian.com/world/2007/apr/28/russia.lukeharding

57. **Harding, Luke**. 2008.: „Abkhazia: Moscow sends troops into second enclave“. The Guardian online. Cit. dne 18. 5. 2015. Dostupné z: http://www.theguardian.com/world/2008/aug/11/georgia.russia

58. **Hathaway, Oona A. et al.** 2012.: „The Law of Cyber-Attack“ In: California Law Review, roč. 100, č. 4

59. **Healey, Jason et al.** 2014.: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Vienna: CCSA. 352 s. ISBN 9780989327404.

60. **Herzog, Stephen.** 2011.: „Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses“ In: Journal of Strategic Studies, podzim 2011, roč. 4, č. 2, s. 49-60.

61. **Hodge, Nathan**. 2009.: „Russian ‘Cyber Militia’ Takes Kyrgyzstan Offline?“ Wired.com. Cit. dne 18. 5. 2015. Dostupné z: http://www.wired.com/2009/01/cyber-militia-t/

62. **Hollis, David**. 2011.: „Cyberwar Case Study: Georgia 2008“ In: Small Wars Journal. Cit dne. 18. 5. 2015. Dostupné z: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

63. **Holsti, Kalevi J.** 1983.: International Politics: A Framework for Analysis, New Yersey: Prentice Hall, Englewood Cliffs. 478 s. ISBN 0134733223.

64. **IRIN**. 2006.: Kyrgyzstan: Economic disparities driving inter-ethnic conflict. Cit. dne 18. 5. 2015. Dostupné z: http://www.irinnews.org/report/33728/kyrgyzstan-economic-disparities-driving-inter-ethnic-conflict

65. **Jackson, Don**. 2009a.: „Kyrgyzstan Under DDoS Attack From Russia: The Cyber Attack No One Is Talking About“. SecureWorks. Cit. dne 18. 5. 2015. Dostupné z: http://www.secureworks.com/resources/blog/research-20957/

66. **Jackson, Don**. 2009b. in Mackey, Robert. 2009.: „Are ‘Cyber-Militias’ Attacking Kyrgyzstan?“ The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?_r=0

67. **Jirásek, Petr a Novák, Luděk a Požár, Josef**. 2013.: Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 200 s., ISBN 9788072513970.

68. **Juhan, Tere**. 2008.: „Russian hackers plan cyber attacks on Baltic countries and Ukraine“. The Baltic Course. Cit. dne 18. 5. 2015. Dostupné z: http://www.baltic-course.com/eng/analytics/?doc=2699

69. **Keizer, Gregg**. 2008a.: „Cyberattacks knock out Georgia's Internet presence“. Computerworld.com. Cit. dne 18. 5. 2015. Dostupné z:

http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html

70. **Keizer, Gregg**. 2008b.: Russian hacker 'militia' mobilizes to attack Georgia. Cit. dne 18. 5. 2015. Dostupné z: http://www.networkworld.com/article/2274800/lan-wan/russian-hacker--militia--mobilizes-to-attack-georgia.html

71. **Keizer, Gregg**. 2009.: Russian 'cyber militia' knocks Kyrgyzstan offline. Cit. dne 18. 5. 2015. Dostupné z: http://www.networkworld.com/article/2262155/lan-wan/russian--cyber-militia--knocks-kyrgyzstan-offline.html

72. **Keller, Bill**. 1991a.: Soviet Crackdown; „Soviet Loyalists in Charge After Attack in Lithuania; 13 Dead; Curfew is Imposed". The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.nytimes.com/1991/01/14/world/soviet-crackdown-soviet-loyalists-charge-after-attack-lithuania-13-dead-curfew.html?pagewanted=all

73. **Keller, Bill**. 1991b.: „Gunmen Kill 6 Lithuania Border Guards". The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.nytimes.com/1991/08/01/world/gunmen-kill-6-lithuania-border-guards.html?scp=12

74. **King, Charles**. 2008.: „The Five-Day War: Managing Moscow After the Georgia Crisis". Foreign Affairs online. Cit. dne 18. 5. 2015. Dostupné z: https://www.foreignaffairs.com/articles/russia-fsu/2008-11-01/five-day-war

75. **Kirk, Jeremy**. 2008.: „Lithuania: Attacks Focused on Hosting Company". PCWorld.com. Cit. dne 18. 5. 2015. Dostupné z: http://www.pcworld.com/article/147960/article.html

76. **Korns, Stephen W. a Kastenberg, Joshua E.** 2009.: „Georgia's Cyber Left Hook" In: Parameters, roč. 38, č. 4, s. 60-76

77. **Kozlowski, Andrzej**. 2014.: „Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan" In: European Scientific Journal 3 (2014). ISSN: 1857 - 7431 (Online).

78. **Kramer, Franklin D. et al.** 2009.: Cyberpower and National Security. Washington: National Defense University Press, xxi, 642 s. ISBN 9781597974233.

79. **Kreč, Luboš a Klang, Mikuláš**. 2015.: „Vláda schválila plán kyberbezpečnosti. Stát bude spolupracovat s firmami“ ze dne 16. 2. 2015. Hospodářské noviny online. Cit. dne 18. 5. 2015. Dostupné z: http://domaci.ihned.cz/c1-63545590-vlada-schvalila-plan-kyberbezpecnosti-stat-bude-spolupracovat-s-firmami

80. **Kuehl, Daniel T.** 2009.: „From Cyberspace to Cyberpower: Defining the Problem“ In: Cyberpower and National Security (eds. Kramer). Washington: National Defense University Press, xxi, 642 s. ISBN 9781597974233.

81. **Kumar, Mohit**. 2012.: „Patriot Hacker ‚The Jester‘ list his all time favorite Open Source Intelligence toolset“. The Hacker News. Cit. dne 18. 5. 2015. Dostupné z: http://thehackernews.com/2012/10/patriot-hacker-jester-list-his-all-time.html

82. **Lachow, Irving.** 2009.: „Cyber Terrorism: Menace or Myth?“ In: Cyberpower and National Security (eds. Kramer). Washington: National Defense University Press, xxi, 642 s. ISBN 9781597974233.

83. **Lemos, Robert**. 2009.: „Cyber attacks disrupt Kyrgyzstan's networks“. SecurityFocus. Cit. dne 18. 5. 2015. Dostupné z: http://www.securityfocus.com/brief/896

84. **Leyden, John**. 2009.: „Russian spy agencies linked to Georgian cyber-attacks“. The Register. Cit. dne 18. 5. 2015. Dostupné z: http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/

85. **Leyden, John**. 2013.: „Patriot hacker 'The Jester' attacks nations offering Snowden help“. The Register. Cit. dne 18. 5. 2015. Dostupné z: http://www.theregister.co.uk/2013/07/04/patriot_hacker_takes_aim_snowden_asylum_candidates/

86. **Libicki, Martin C**. 2007.: Conquest in Cyberspace. Cambridge: Cambridge University Press. 336 s. ISBN: 0521692148

87. **Libicki, Martin C**. 2009.: Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND, xxiv, 214 s. ISBN 9780833047342.

88. **Limnell, Jarno**. 2014.: „Why hasn’t Russia unleash a cyber attack on Ukraine?“ CBSNews online. Cit. dne 18. 5. 2015. Dostupné z: http://www.cbsnews.com/news/why-hasnt-russia-unleashed-a-cyber-attack-on-ukraine/

89. **Lorents, Peeter a Ottis, Rain**. 2010.: Knowledge Based Framework for Cyber Weapons and Conflict. Tallinn: CCD COE Publications.

90. **Luht, Lauri**. 2014. E-government, M-government security, questions and answers. Panel konference Information Security and Cyber Defence, 7. – 8. září 2014, Budapešť.

91. **Macek, Jakub**. 2003.: „Kyberprostor (Cyberspace)“ In: Revue pro Média, č. 5. Cit. dne 18. 5. 2015. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm

92. **Mackey, Robert**. 2009.: „Are ‘Cyber-Militias’ Attacking Kyrgyzstan?“ The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?_r=0

93. **Mamatov, Arslan**. 2009.: „Kyrgyzstan: Government Targets Opposition“. Eurasianet.org. Cit. dne 18. 5. 2015. Dostupné z: http://www.eurasianet.org/departments/insightb/articles/eav012109a.shtml

94. **Mareš, Miroslav**. 2012.: Paramilitarismus v České republice. Brno: Centrum pro studium demokracie a kultury. 316 s. ISBN 978-80-7325-297-7.

95. **Markoff, John**. 2008.: „Before the Gunfire, Cyberattacks“. The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.nytimes.com/2008/08/13/technology/13cyber.html

96. **Martínez, Israel**. In: Violino, Bob. 2013: Unseen, all-out cyber war on the U.S. has begun. Cit. dne 18. 5. 2015. Dostupné z: http://www.infoworld.com/article/2612825/hacking/unseen--all-out-cyber-war-on-the-u-s--has-begun.html

97. **Maskeliunas, Saulius a Otas, Alfredas**. 2008.: Development and Application of Information Society Strategies in Lithuania. Prezentace. Cit. dne 18. 5. 2015. Dostupné z: http://www.scholze-simmel.at/it_star/ws3/lithuania_ppt.pdf

98. **Maurer, Tim.** 2013.: „SOLAR SUNRISE: Cyber Attack from Iraq?“ In: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (eds. Healy). Vienna: CCSA. 352 s. ISBN 9780989327404.

99. **McLaughlin, Daniel**. 2008.: „Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites“. The Irish Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155

100. **Milashina, Elena**. 2014.: „Russia intensifies restrictions on blogs, social media“. Committe to Protect Journalists. Cit. dne 18. 5. 2015. Dostupné z: https://cpj.org/blog/2014/07/russia-intensifies-restrictions-on-blogs-social-me.php

101. **Moeller, Bjorn**. 2003: Conflict Theory. Aalborg: Institut for Historie, Internationale Studier og Samfundsforhold, Aalborg Universitet.

102. **Monaghan, Andrew**. 2009.: „Russian Foreign and Security Policy – A Strategic Overhaul?“ In: Security Politics in Asia and Europe (Hofmeister, Wilhelm eds.). 2010. Singapur: Konrad-Adenauer-Stiftung.

103. **Morrison, Aimée H**. 2009.: An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace' In: New Media & Society, February/March 2009, roč. 11, č. 1-2, s. 53-71.

104. **Mulvenon, James C. a Rattray, Gregory J.** 2012.: Adressing Cyber Instability: Executive Summary. 38 s. ISBN: 9781105546228.

105. **Myers, Steven Lee**. 2007a.: „Russia Rebukes Estonia for Moving Soviet Statue“. The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html?em&_r=0

106. **Myers, Steven Lee**. 2007b.: „TALLINN JOURNAL; Debate Renewed: Did Moscow Free Estonia or Occupy It?“ The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: query.nytimes.com/gst/fullpage.html?res=9402E6DB163FF936A15752C0A9619C8B63&pagewanted=2

107. **NATO**. 2011.: Konečné stanovisko setkání Severoatlantické Rady na úrovni ministrů zahraničních věcí dne 7. prosince 2011, Brusel. Cit. dne 18. 5. 2015. Dostupné z: http://www.nato.int/cps/en/natolive/official_texts_81943.htm?mode=pressrelease

108. **Nazario, Jose**. 2009.: Kyrgyzstan DDoS Attacks. Cit. dne 18. 5. 2015. Dostupné z: http://www.arbornetworks.com/asert/2009/02/kyrgyzstan-ddos-attacks/

109. **Paganini, Pierluigi**. 2013.: „Is RBN (Russian Business Network) Really Linked to Facebook Zeus Variant?“ Cyber Defense Magazine. Cit. dne 18. 5. 2015. Dostupné z: http://www.cyberdefensemagazine.com/is-rbn-russian-business-network-really-linked-to-facebook-zeus-variant/

110. **PC Tools**. 2008.: Cyber crooks attack Lithuanian websites. Cit. dne 18. 5. 2015. Dostupné z: http://www.pctools.com/industry-news/article/cyber_crooks_attack_lithuanian_websites-18663956/

111. **Plakans, Andrejs**. 2011.: A concise history of the Baltic States. Cambridge: Cambridge University Press, 2011, xvi, 472 s., ISBN 9780521833721

112. **Pšeja, Pavel.** 2002.: „Konflikt“ In: Česká bezpečnostní terminologie (eds. Zeman). Brno: Mezinárodní politologický ústav.

113. **Putin, Vladimir**. 2014.: Projev na společném zasedání ruského parlamentu. Neoficiální přepis. Cit. dne 18. 5. 2015. Dostupné z: http://www.washingtonpost.com/world/transcript-putin-says-russia-will-protect-the-rights-of-russians-abroad/2014/03/18/432a1e60-ae99-11e3-a49e-76adc9210f19_story.html

114. **Rattray, Gregory J.** 2001.: Strategic Warfare in Cyberspace. Cambridge: MIT Press. 527 s. ISBN: 0262182092.

115. **Rattray, Gregory J. a Healey, Jason**. 2011.: „Non-state Actors and Cyber Conflict“ In: America’s Cyber Future: Security and Prosperity in the Information Age (Lord, Kristin M. a Sharp, Travis eds.). Cit. dne 18. 5. 2015. Dostupné z: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=129907

116. **Reuters.** 2008.: Lithuanian tax office website hit by cyber attack. Cit. dne 18. 5. 2015. Dostupné z: http://www.reuters.com/article/2008/07/21/lithuania-web-attacks-idUSMAR14153920080721

117. **Rhoads, Christopher**. 2009.: „Kyrgyzstan Knocked Offline“. Wall Street Journal online. Cit. dne 18. 5. 2015. Dostupné z: http://www.wsj.com/articles/SB123310906904622741

118. **Rhodin, Sara**. 2008.: „Hackers Tag Lithuanian Web Sites With Soviet Symbols“. The New York Times online. Cit. dne 18. 5. 2015. Dostupné z: http://www.nytimes.com/2008/07/01/world/europe/01baltic.html?_r=1&

119. **Rid, Thomas**. 2013.: Cyber war will not take place. London: Hurst & Company, xvi, 218 s. ISBN 9781849042802.

120. **Richards, Jason**. 2009.: Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. Portál International Affairs Review. Cit. dne 18. 5. 2015. Dostupné z: http://www.iar-gwu.org/node/65

121. **Roudik, Peter**. 2008.: Lithuania: Ban on Nazi and Soviet Symbols. Library of Congress online. Cit. dne 18. 5. 2015. Dostupné z: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l20540487_text

122. **Ruská Federace**. 2000. Doktrína informační bezpečnosti Ruské federace. Neoficiální překlad. Cit. dne 18. 5. 2015. Dostupné z: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

123. **Ruská Federace**. 2009. Strategie národní bezpečnosti Ruské federace do roku 2020. Neoficiální překlad. Cit. dne 18. 5. 2015. Dostupné z: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020

124. **Saad, Sabrine a Bazan, Stéphane B. a Varin, Christophe**. 2011.: Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield. Cit. dne 18. 5. 2015. Dostupné z: http://www.websci11.org/fileadmin/websci/posters/96_paper.pdf

125. **Sapetkaite, Vaiva**. 2012.: „Cybernetic (in)security: situation in the Baltic States“. Geopolitika. Cit. dne 18. 5. 2015. Dostupné z: http://www.geopolitika.lt/?artc=5541

126. **Schmitt, Michael.** 2015.: Preparing for Cyber War: A Clarion Call. *Just Security.* Cit. Dne 18. 5. 2015. Dostupné z: http://justsecurity.org/21361/preparing-cyber-war-clarion-call/

127. **Schmitt, Michael eds**. 2013.: Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press. 304 s. ISBN: 1107024439.

128. **Schmitt, Michael a Vihul, Liis**. 2014.: „Proxy Wars in Cyberspace: The Evolving International Law of Attribution“ In: Fletcher Security Review, Jaro 2014, roč. 1, č. II.

129. **Schneier, Bruce**. 2007.: Cyberwar: Myth or Reality?. Cit. dne 18. 5. 2015. Dostupné z: https://www.schneier.com/essays/archives/2007/11/cyberwar_myth_or_rea.html

130. **Secure Works**. 2008. „Compromised US and Chinese Computers Launch Greatest Number of Cyber Attacks, according to SecureWorks' Data.“ Tisková zpráva ze dne 22. září 2008. Cit. dne 18. 5. 2015. Dostupné z: http://www.secureworks.com/media/press_releases/20080922-attacks

131. **Shackelford, Scott J.** 2009.: „From Nuclear War to Net War: Analogizing Cyber Attacks in International Law“ In: Berkley Journal of International Law (BJIL), roč. 25, č. 3

132. **Shein, Rob**. 2010.: A Brief Summary of Cyber Warfare. Cit. dne 18. 5. 2015. Dostupné z: http://www.infosectoday.com/Articles/Cyber-Warfare.htm

133. **Singer, P.W. a Friedman, Allan.** 2014.: Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, viii, 306 s. ISBN 9780199918096

134. **Space War.** 2007.: Russian Officials Tout Iskander MIRV As 21st Century ABM Buster. Cit. dne 18. 5. 2015. Dostupné z: http://www.spacewar.com/reports/Russian_Officials_Tout_Iskander_MIRV_As_21st_Century_ABM_Buster_999.html

135. **Spiegel Online.** 2007.: Deadly Riots in Tallinn: Soviet Memorial Causes Rift between Estonia and Russia. Cit. dne 18. 5. 2015. Dostupné z: http://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html

136. **Sputnik News**. 2008.: RIA Novosti hit by cyber-attacks as conflict with Georgia rages. Cit. dne 18. 5. 2015. Dostupné z: http://sputniknews.com/russia/20080810/115936419.html

137. **Stewart, Susan**. 2014.: „The EU, Russia and a Less Common Neighbourhood" In: SWP Comments, Leden 2014. 8 s. Cit. dne 18. 5. 2015. Dostupné z: http://www.swp-berlin.org/en/publications/swp-comments-en/swp-aktuelle-details/article/eu_russland_und_oestliche_partnerschaft.html

138. **STRATFOR.** 2009.: Russia: Protecting Citizens Living Abroad. Analýza ze dne 2. prosince 2009. Cit. dne 18. 5. 2015. Dostupné z: https://www.stratfor.com/analysis/russia-protecting-citizens-living-abroad

139. **Šmíd, Tomáš et kol.** 2010.: „Vybrané konflikty o zdroje a suroviny" Brno: Masarykova Univerzita.

140. **The Economist**. 2007a.: The truth about eSStonia. Cit. dne 18. 5. 2015. Dostupné z: http://www.economist.com/node/9645274

141. **The Economist.** 2007b.: Estonia has faced down Russian rioters. But its websites are still under attack. Cit. dne 18. 5. 2015. Dostupné z: http://www.economist.com/node/9163598

142. **The Economist**. 2013.: Greetings to the President. Cit. dne 18. 5. 2015. Dostupné z: http://www.economist.com/blogs/easternapproaches/2013/06/lithuania-under-cyber-attack

143. **The Moscow Times**. 2013. Lavrov Blasts 'Vote Theft' at Eurovision. Cit. dne 18. 5. 2015. Dostupné z: http://www.themoscowtimes.com/arts_n_ideas/article/lavrov-blasts-vote-theft-at-eurovision/480278.html

144. **Thomas, Timothy L**. 2009.: Nation-state Cyber Strategies: Examples from China and Russia. (eds. Kramer). Washington: National Defense University Press, xxi, 642 s. ISBN 9781597974233.

145. **Tikk, Eneken a Kaska, Kadri a Vihul, Liis**. 2010.: International Cyber Incidents: Legal Considerations. Tallinn: CCD COE Publications.

146. **US CCU – United States Cyber Consequences Unit.** 2009.: Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. Cit. dne 18.

5. 2015. Dostupné z: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

147. **USA Today**. 2008.: Russia warns Lithuania against U.S. missile defense sites. Cit. dne 18. 5. 2015. Dostupné z: http://usatoday30.usatoday.com/news/world/2008-07-02-Russia-missile-defense_N.htm

148. **Valeriano, Brandon**. 2013.: Becoming Rivals: The Process of Interstate Rivalry Development. London: Routledge. 168 s. ISBN-10: 0415537533.

149. **Valeriano, Brandon a Maness, Ryan C.** 2014.: „The dynamics of cyber conflict between rival antagonists, 2001-11“ In: Journal of Peace Research, roč. 51, č. 3, s. 347-360.

150. **Vláda ČR**. 2014.: Národní strategie kybernetické bezpečnosti pro období let 2015 až 2020.

151. **Vláda Kanady**. 2010.: Kanadská strategie kybernetické bezpečnosti. Cit. dne. 18. 5. 2015. Dostupné z: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

152. **Wild, Natalie**. 2008.: „Does A State Have The Right To Protect Its Citizens Abroad?“ Radio Free Europe online. Cit. dne 18. 5. 2015. Dostupné z: http://www.rferl.org/content/Does_A_State_Have_The_Right_To_Protect_Its_Citizens_Abroad/1193050.html

153. **Yasmann, Victor**. 2007.: „Russia: Monument Dispute With Estonia Gets Dirty“. Radio Free Europe online. Cit. dne 18. 5. 2015. Dostupné z: http://www.rferl.org/content/article/1076297.html

154. **Zeman, Petr et al**. 2002.: Česká bezpečnostní terminologie. Brno: Mezinárodní politologický ústav.

155. **Zimet, Elihu a Skoudis, Edward**. 2009.: „A Graphical Introduction to the Structural Elements of Cyberspace“ In: Cyberpower and National Security (eds. Kramer). Washington: National Defense University Press, xxi, 642 s. ISBN 9781597974233.