UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií

Lukáš Jandura

Možnosti zlepšení strategií pro kybernetickou bezpečnost

Diplomová práce

Praha 2016

Autor práce: **Mgr. Lukáš Jandura**

Vedoucí práce: **PhDr. Vít Střítecký, M.Phil.**

Bibliografický záznam

JANDURA, Lukáš. *Možnosti zlepšení strategie kybernetické bezpečnosti.* Praha, 2016. 77 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut politologických studií. Katedra bezpečnostních studií. Vedoucí diplomové práce PhDr. Vít Střítecký, M.Phil.

Anotace (abstrakt)

Práce se zaměřuje na dynamiku centrálních uzlů v kyberprostoru jako klíčových struktur bezpečnosti v této doméně. Daný přístup vycházející z teorie sítí Alberta-László Barabásiho je konceptualizován společně s kyberprostorem v bezpečnostních studiích a rolí státu v něm. Hlavní výzkumná otázka týkající se zlepšení strategií kybernetické bezpečnosti je zodpovězena strukturovaným výčtem možností, ke kterým by měl stát ve strategii zaujmout postoj a tím vyjasnit svou pozici vůči centrálním uzlům; zda do nich bude v budoucnu zasahovat, v jakých mezích a jaké prostředky je ochoten využít při snaze ovlivnit uzly, nad nimiž nemá přímou kontrolu.

Abstract

The thesis focusses on central nodes' dynamics in cyberspace, representing its key elements. Such approach derives from the theory of networks developed by Albert-László Barabási and it is conceptualised along with cyberspace in security studies and the role of a state in cyberspace. Main question, which is how to improve cybersecurity strategies, is answered by well-structured package of possible positions of a state towards central nodes. It asses the level of involvement in cyberspace, boundaries of intrusion into central nodes and acceptable tools usable against those which are not directly accessible.

Klíčová slova

Kyberprostor, uzly, vazby, centra, kybernetická bezpečnost, kybernetická obrana, bezškálové sítě, decentralizace, strategie kybernetické bezpečnosti, bezpečnost, bezpečnostní studia, Barabási

Keywords

Cyberspace, nodes, links, cybersecurity, cyberdefence, scale-free networks, decentralization, cybersecurity strategy, security, security studies, Barabási

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.

2. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 23. 7. 2016 Lukáš Jandura

Poděkování

Na tomto místě bych rád poděkoval především svému vedoucímu diplomové práce panu **PhDr. Vítu Stříteckému, M.Phil.** vytrvalou podporu při vytváření práce a rozšíření obzorů poznání.

Rovněž bych rád poděkoval panu **Mgr. Nikolovi Schmidtovi** za konzultace a inspiraci při zpracování tématu a svěží vhled do problematiky.

Díky směřuje také panu **Mgr. Martinu Kolombovi** za nasměrování při pátrání po odlišných pohledech na fenomén kyberprostoru a za sdělené zkušenosti z praxe a paní **Mgr. Kláře Novákové** za zpětnou vazbu k tématům práce.

Na závěr patří poděkování také členům projektové skupiny „**Customs against Internet Crime**“ za bezprostředně předávané zprávy o kauzách v kyberprostoru.

Obsah

Úvod

Kyberprostor se stal trvalou součástí našeho každodenního života. Plně prostupuje téměř všemi lidskými činnostmi. Tato nová realita prostupuje všemi kontinenty, počítači, mobilními telefony, průmyslovými stroji, automobily, vybavením domácností, ale i jadernými elektrárnami a zbraněmi, či sociálními skupinami, státy, nevládními a mezinárodními organizacemi a jednotlivci. Kyberprostor patří mezi základní součást moderní společnosti, a státy proto vyvíjejí činnosti za účelem zvýšení jeho bezpečnosti.

Takto rozsáhlý prostor, zatím bez dlouhé historie, jež by nás s ním naučila bezpečně zacházet, nutně generuje nová rizika a hrozby. Obrana proti nim je aktuální téma a přístupů může být mnoho. Cílem této práce je jeden z těchto přístupů nastínit a prozkoumat jeho možné přispění k bezpečnosti informačních sítí. Bezpečnost kyberprostoru již není pouze záležitost inženýrů, programátorů či administrátorů, ale stala se rovněž odpovědností vojáků, politiků a diplomatů.[1]

Práce nepřináší konkrétní opatření, které by bylo možné do kybernetické strategie jednoduše vložit. Cílem je otevřít cestu, jak přemýšlet nad některými oblastmi, které upravují, nebo by měly upravovat, strategie kybernetické bezpečnosti. Práce k problému přistupuje optikou teorie sítí Alberta-László Barabásiho[2] a jeho poznatky ze studia bezškálových sítí.

Důležitost uzlů popsaná Barabásim vedla k tezi, stojící u vzniku této práce. Záměrem bylo zkoumat, jak jsou tato centra zmiňována v kybernetických strategiích bezpečnosti jednotlivých států či celků (např. Evropské unie), jak se tyto strategie kybernetické obrany vypořádávají s důležitostí center, s jejich ochranou a rolí v kyberprostoru. Hypotéza předpokládala, že jejich role má zřejmě mnohem větší dopad na bezpečnost kyberprostoru, než jen ochrana uzlů samotných. Ohrožení daného centrálního uzlu je pro síť bezpochyby nebezpečné, ale celá problematika je

[1] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 148

[2] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. str. 122.

komplexnější. Vycházíme-li z práce Barabásího, funkce center v síti je zcela klíčová, a proto byl předpoklad, že centra zásadním způsobem ovlivňují téměř celou doménu kyberprostoru.

Práce nejprve pátrala po ustanoveních a obratech ve vybraných strategiích kybernetické bezpečnosti, nedařilo se v nich však identifikovat uchopení, kterým by k uzlům přistupovaly. Bylo zjištěno, že pro účely práce k nim strategie přistupují až příliš obecně či naopak příliš konkrétně (jmenovitě), a nedařilo se proto nalézt v jednotlivých strategiích kybernetické bezpečnosti nějaký více teoretický či strategický přístup k centrálním uzlům, který by z pohledu bezpečnostních studií přinášel zajímavý vědecký výsledek. Kybernetické strategie neposkytují dostatečně zajímavou odlišnost jednotlivých uzlů a neposkytují vodítko, jak k centrům přistupovat. Autoři strategií kybernetické bezpečnosti[3] při zpracování těchto dokumentů obvykle upravují jen část problematiky. A nelze jim to vyčítat, neboť své práce píší za jiným účelem, než je teoretické rozpracování tématu uzlů v kyberprostoru. Po delším zkoumání dospěl autor k rozhodnutí, že tato cesta nepovede k užitečnému výsledku a rozhodl se pozměnit záměr práce. Vznikla tak myšlenka analyzovat roli center v těchto reálných sítích hlouběji. Udělat krok zpět a provést vlastní analýzu přínosu či naopak rizik center pro bezpečnost kyberprostoru.

Struktura práce

Práce se ptá na otázky spojené s rolí centrálních uzlů a jejími dopady na kyberprostor jako na sociální prostředí.

- Jaká je úloha center v kyberprostoru?
- Jak je možné jejich zkoumáním vylepšit kybernetickou bezpečnost?
- Jak by měl stát k centrům přistupovat?

[3] Např. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-05-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

Všechny tyto otázky vedou k výzkumnému záměru práce, kterým je hledání možností zlepšení strategií kybernetické bezpečnosti, zaměříme-li se na centra jako na významné aktéry kyberprostoru.

Struktura práce začíná představením Barabásiho teorie o uzlech a vazbách v bezškálových sítích[4] a z ní vyplývající význam center v kyberprostoru. Typický pro tyto sítě je růst a preferenční připojování nových vazeb právě k centrům. Růst center proto vede k určité centralizaci sítě a stoupá jejich vliv v síti.

Poté práce konceptualizuje kyberprostor v oboru bezpečnostních studií a následně roli státu a jeho zasahování do kyberprostoru. Dále zkoumá, zda by se měl stát na centra více koncentrovat a vymezit si, jakou roli bude hrát při jejich kontrole. A *kontrola* je zde myšlena především v jejím druhém významu. Tedy nikoli jako *kontrola dodržování nařízených bezpečnostních opatření (audit),* jež mají bránit centra proti kybernetickým útokům, ale především *kontrola ve smyslu vlivu nad centry*, schopnosti jejich ovládání či působení na ně tak, aby bylo jejich fungování v souladu s národními zájmy. Zkrátka se ptá, jak mít centra *pod kontrolou*.

Práce poté pojednává o možném vlivu státu na centra, a jaký k nim může zaujímat vztah – zda budou zcela nezávislé, zda budou upraveny zákony, zda je bude stát dozorovat nezávislými nebo státními orgány, zda je bude využívat pro své zájmy či je přímo bude provozovat. Jak má stát postupovat, pokud nad centrem nemá nebo ztratí kontrolu a je pro něj nedosažitelné? Buď proto, že je vůči státu autonomní (patří nespolupracujícímu soukromému subjektu) nebo je dané centrum pod vlivem jiného státu (či přímo mimo území).

Následně je analyzována současná situace ohledně postojů, které státy dosud zastávají vůči centrům. Prostřednictvím konkrétních příkladů je naznačeno, jak státy přistupují k velkým soukromým centrům (nutí je například spolupracovat s tajnými službami) a jak kvůli tomu vlastně ohrožuje svůj monopol na bezpečnost.

---

[4] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 75.

Závěrem jsou shrnuty přístupy, jak by se stát měl ve strategii kybernetické bezpečnosti vymezit vůči centrům, a definovat svůj přístup v otázce zásahu státu do kyberprostoru a do jednotlivých center. Výzvou pro stát zůstává, zda ve strategiích definovat kroky, které podnikne, pokud centra nebudou spolupracovat, a které přijme za účelem regulace center a jejich činnosti (zda jim například zakáže vývoz „kybernetických zbraní“). V neposlední řadě se práce připojuje k apelu, aby se na daném postoji sjednotilo více států a šířili tento pohled jako standard liberálních demokracií globálně.

Výběr tématu a zdrojů

Dané téma bylo zvoleno z více důvodů. Jedním z nich je aktuálnost tohoto tématu a potřeba jej řešit, neboť jeho překotný vývoj, globální rozměr a obrovské množství aktérů vytvořily zcela specifický a komplexní systém, Dá se nazvat až organickým a lze na něj nahlížet různými paradigmaty. Druhým důvodem je, že vzhledem k velkému dopadu tématu bezpečnosti v kyberprostoru na fungování společnosti a na každodenní činnost lidí je mu věnována patřičná mediální a vědecká pozornost a to i přes nutnost určité technické vědomostní báze, se kterou je třeba k němu přistupovat, a kvůli čemuž může být pro sociální vědy hůře uchopitelný. Momentálně je proto výzvou se tomuto tématu věnovat. Přesto existuje možnost, že za pár let nebude kyberprostor představovat velký důvod ke zkoumání. Všechna jeho současná rizika mohou být v budoucnu eliminována novými technologiemi a standardy, ač třeba na úkor jeho svobody.

Podkladem pro práci je nejznámější odborná literatura na téma kyberprostoru, která různým způsobem kyberprostor jako takový rozvíjí, nahlíží na něj různými pohledy a poskytuje tím podklad pro aplikaci Barabásiho teorie. Důležité jsou také samozřejmě strategie kybernetické bezpečnosti. Sekuritizace kyberprostoru na vládní úrovni probíhá především prostřednictvím strategických a politických dokumentů, které mohou být zatíženy různými relikty ze strategií, určených pro jiná odvětví, případně předsudky, předpoklady a sociálními konstrukty, které nemusí být pro kyberprostor, jakožto nový prostor, jež nemá pro laika zcela očividné zákonitosti, vhodné. Jedním z úkolů práce je nabídnout odlišný pohled na problematiku a tím se pokusit odhalit nové výzvy, či řešení současných problémů. Záměrem práce je pokusit se uchopit kyberprostor odlišně, než tomu bylo doposud a přijít s myšlenkami, které jeho chápání dále rozvíjí. V návaznosti na to je možné jej vnímat v širším kontextu a poskytnout čtenáři neotřelý pohled.

Vysvětlení pojmů

Následující oddíl má za úkol čtenáře seznámit se základními pojmy, vyskytujícími se v této práci, a především s významem těchto pojmů tak, jak jsou v práci chápány. Jasné vymezení je pro účely práce nezbytné, neboť jen tak lze dostatečně rozlišit některé hlavní rozdíly v jednotlivých řešeních.

Bezškálové a reálné sítě

Bezškálové sítě jsou v práci chápány tak, jak je definuje A. L. Barabási. Jsou to sítě, kde neexistuje nějaká škála či typický představitel uzlu, který by síť reprezentoval. Naopak rozdělení počtu vazeb (tedy konektivity) u jednotlivých uzlů odpovídá mocninnému zákonu. „Pomalu klesající mocninné rozdělení přirozeným způsobem vyjadřuje, že tyto vysoce propojené anomálie jsou poměrně častým jevem. Předpovídá, že každá bezškálová síť bude mít několik velkých center, která budou zásadním způsobem předurčovat topologii sítě.“[5] Bezškálové sítě jsou řízeny dvěma zákony: růstem a preferenčním připojováním, což bude dále rozvíjeno a byly objeveny právě díky internetu.[6] Typickým představitelem takové sítě je právě kyberprostor.

Decentralizovaná síť

Decentralizovanou síť chápe Barabási (stejně jako tato práce) ve své knize poněkud odlišně, než by bylo se zdálo logické. Při použití negativního vymezení můžeme říci, že nejde o síť zcela bez center. Takovou (připomínající například rybářkou síť) pojmenovává rozptýlenou sítí.[7] Naopak centralizovaná síť má pouze jedno velké centrum a je nazvána sítí hierarchickou. Decentralizovaná síť pak znamená, že jde o síť bezškálovou, u které je několik významných center, které na sebe mají navázánu většinu uzlů. Rozdělení konektivity dalších uzlů pak klesá dle mocninného zákona. Zástupcem decentralizované sítě dle této definice je právě kyberprostor. Lze také říci, že pro účely této práce se pojmy bezškálová síť a decentralizovaná síť shodují, ač každý klade důraz na jinou vlastnost těchto sítí.

---

[5] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 75.
[6] Ibid. s. 140.
[7] Příloha 1

Reálné sítě

Bezškálové sítě představují ideální model. Mají matematicky vyjádřitelné rozdělení konektivity, schopnost samoorganizace a je jim vlastní růst a preferenční připojování. Takovou síť však v reálném světě nehledejme. Situace je mnohem komplikovanější, jednotlivé uzly se mohou v čase zmenšovat, měnit své vazby, či úplně zanikat. Jednotlivé celky se mohou sítí pohybovat či se mohou do sítě promítat další zákony, se kterými ideální model bezškálové sítě nepočítá. Abychom rozlišili, zda mluvíme o tomto ideálním modelu, ve kterém se vše odvíjí matematicky přesně, nebo o realitě (která je navíc v případě kyberprostoru ovládaná, vytvářená a tvarovaná uměle lidmi), nazýváme tyto sítě reálnými (případně komplexními). Pro účely této práce bude pojmem reálná či komplexní síť vždy myšlena síť, která má za svůj ideální model síť bezškálovou. Nutno také dodat, že aplikace Barabásiho zákonů platných pro ideální sítě na sítě reálné může vést k opomenutí důležitých vlastností těchto reálných sítí a tím k deformaci závěrů z takové aplikace vzešlých.

Kyberprostor, internet a world wide web

Otázka, jak uchopit pojem kyberprostor v bezpečnostních studiích je součástí této práce a bude obsahem dalšího textu. Je však vhodné na začátku upozornit na odlišnost pojmů kyberprostor, internet a world wide web. Zatímco kyberprostor je široký pojem, zahrnující většinu myslitelných technických prvků propojených do sítě, která umožňuje komunikaci a interakci lidí a tím jim poskytuje sociální realitu, pojmy internet a world wide web jsou v práci chápány mnohem úžeji.[8]

Internet představuje soustavu prvků technické infrastruktury včetně koncových stanic a umožňuje výměnu informací mezi těmito prvky v binárním kódu. Jsou to všechny servery, směrovače, optické kabely, datová centra apod. World wide web je pak síť, složená (víceméně) pouze z webových stránek a jednotlivých služeb, které tyto stránky

[8] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. str. 146.

poskytují (od e-mailových klientů přes sociální sítě až po online stream videa). Internet i world wide web jsou tedy podmnožinou kyberprostoru.

Libicki poněkud mylně uvádí, že internet se rovná kyberprostoru („vše připojené na internet je připojené do kyberprostoru, a tedy sám kyberprostor.“[9]), avšak je za to Bryantem kritizován, neboť snadno pak může dojít k ignorování sítí, které nejsou přímo do internetu zapojeny, ale pravidla kyberprostoru pro ně rovněž platí.[10]

(Kybernetické) strategie

Tento pojem je v práci vnímán jako nadřazený pojem pro politické dokumenty, které jsou pravidelně vydávány jednotlivými státy, či seskupeními za účelem budování kapacit pro zvládání (kybernetických) hrozeb a přípravy na ně. Pokud není řečeno jinak, jde vždy o strategie kybernetické bezpečnosti. V některých případech však práce k tomuto pojmu přistupuje také obecně jako ke strategii, přinášející způsoby, jak se vypořádat s bezpečnostními riziky v kyberprostoru; bez návaznosti na písemně zpracovaný politických dokument.

[9] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 323

[10] BRYANT, William D. International Conflict and Cyberspace Superiority: Theory and Practice Routledge Studies in Conflict, Security and Technology, Routledge, 2015, ISBN 1317420381, 9781317420385

Východiska práce

Současný mezinárodní diskurz na téma kyberprostor je z velké části zaměřen především na chování států v oblasti kyberprostoru a použití síly. Nestátní aktéři často stojí mimo dosah mezinárodních úmluv a dohod.[11]

Význam kyberprostoru a jeho bezpečnosti vystihuje i následující citace: „*Kybernetická bezpečnost se postupně stává jednou z priorit národních bezpečnostních politik a mezinárodní agendy organizací, jako je Severoatlantická aliance a Evropská unie. Je možné, že se jednou stane prioritou hlavní.*“ Nabízí se otázka, zda je vůbec diskurz, uvedený v těchto větách, nastaven správně. Nemělo by být prioritou například zkoumání role transnacionálních entit, které kyberprostor využívají a stávají se pro jeho bezpečnost klíčové? Uvedené prohlášení je s nadsázkou podobné, jako bychom říkali, že prioritou národní bezpečnostní politiky jsou veřejné prostory. Ale co se v těchto prostorech odehrává, opomíjíme.

U národních států lze pozorovat rozpolcenost. Na jedné straně se snaží o vytvoření bezpečného kyberprostoru a o ochranu kritické infrastruktury. Odvrácenou stranou je však snaha udržet současný stav, který jim umožňuje bezprecedentní možnosti sledování, propagandy, přesně cílených sabotáží, a tedy i šanci získat strategickou výhodu nad nepřítelem. V tomto směru vlastně hrají státy role aktérů nestátních.[12]

Technologie sice není to jediné, co tvoří kyberprostor, výrazně však zasahuje do způsobu jeho používání. A především v sobě problematika bezpečnosti kyberprostoru obsahuje přemýšlení o použití technologie jako takové.[13] Ta vytváří zcela nový způsob sociální interakce, případně konfliktu. Články zaměřené na bezpečnost mají tendenci dívat se na kyberprostor právě z technického hlediska. Takový pohled přináší sám o sobě určité problémy, protože toto zaměření zužuje šířku vhledu do problematiky a práce tak nemohou poskytnout kompletní definici kyberprostoru.[14] Současná úroveň znalostí často

---

[11] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 77
[12] Ibid. s. 77
[13] Ibid. s. 70-71
[14] Ibid. s. 71

nevede k poznáním, která by pomohla vytvořit účinnou strategii k vyřešení některých otázek bezpečnosti kyberprostoru, protože pouze aplikuje znalosti z jiných lidských oblastí. Ty však nelze tak jednoduše na doménu kyberprostoru použít. Tak vznikla prvotní myšlenka této práce – přinést prostřednictvím Barabásiho teorie bezškálových sítí nový pohled na kyberprostor a jeho roli v mezinárodní bezpečnosti. Tedy zkoumat sociální konstrukt kyberprostoru z pohledu center a jejich rolí.

I tato práce se zabývá úzkou výsečí kybernetické bezpečnosti týkající se významu velkých uzlů. Ty vnímá v širším pojetí, kdy nezahrnuje pouze systémy důležité pro chod státu, ale všechna velká centra v kyberprostoru, jak fyzická, tak virtuální a snaží se zkoumat jejich bezpečnost v širokém pojetí od bezpečnosti, přes jejich vliv a možnost jejich kontroly.

Mluvíme-li o typologii kyberprostoru, je možné zvolit různé přístupy, jichž byla zpracována celá řada. Kyberprostor lze vnímat různými pohledy, pro něž byl zvolen sjednocující pojem **náhled**. V další části tak budou analyzovány jednotlivé náhledy na kyberprostor a roli centrálních uzlů v těchto náhledech.

Ač budou možná některé komentáře v této práci působit kriticky, autor věří, že právě prostřednictvím kritického myšlení je možné se věcně bavit o samé podstatě věcí a jejich reálném přínosu. Smyslem kritických komentářů je položit otázky otevírající diskuzi a nabízející pohled z druhé strany.

Původní záměr práce

Prvotní výzkumný plán nevedl ke smysluplnému výsledku a bylo třeba jej upravit. Záměr cílil na detailní prozkoumání teorie sítí od A. L. Barabásiho a zvolení prvků, které jsou relevantní pro zkoumání kyberprostoru a možností jeho obrany. Z teorie měla být použita především role center a jejich důležitost v bezškálových sítích a dále možnosti jak takovou síť prostřednictvím center ohrozit či jak působit na centra tak, aby se zvyšovala jejich atraktivita (zdatnost) pro ostatní uzly v síti.

Původní výzkumná otázka zněla: Jaké jsou možnosti zlepšení v oblasti obrany proti kybernetickým hrozbám? Tato otázka byla v současné podobě práce rozšířena o roli uzlů v oblasti kybernetické bezpečnosti.

Plánovaným cílem bylo zkoumat, zda jsou současné strategie boje proti kybernetickým hrozbám dostatečné, zda je možné v nich nalézt nedostatky, které jsou způsobeny nesprávným přístupem k této oblasti, jak tyto nedostatky případně odstranit a jakým směrem by mohla vést jiná cesta k obraně proti kybernetickým hrozbám. Ač bylo možné v těchto strategiích jednotlivé uzly do jisté míry vyhledat, jak už bylo zmíněno, bylo velmi složité z nich vytvářet smysluplné závěry. Označení uzlů bylo buď příliš obecné, nebo naopak příliš konkrétní. A především, jejich analýzou nebylo možné odpovědět na otázku, zda a jaké nedostatky by mohla teorie sítí odstranit. Kybernetické strategie totiž mají omezené styčné plochy s teoretickou politologií a tak konkrétní zlepšení tento způsob výzkumu nepřinášel.

Jako původní metoda pro zhotovení práce byla vybrána případová studie se třemi případy, ukotvená do teoretického konceptu již zmíněné teorie sítí dle Alberta-László Barabásiho, kterou měl být podpořen ideální model - strategie decentralizace. Mělo vzniknout určité „předporozumění“ podobně jako v principu hermeneutického kruhu.[15] Toto předporozumění je relevantní i pro současnou podobu práce, neboť právě analýzou Barabásiho teorie vzniklo předporozumění o centrech a jejich smyslu v síti, které bylo postupně aplikováno na různé fenomény, které se v kyberprostoru vybírali.

Zamýšlený záměr práce předpokládal provedení hloubkové analýzy bezpečnostních strategií vydaných k zabezpečení kyberprostoru v posledních 5 letech, zohledňující kontext (sociální, politický, historický) a poskytující komplexní obrázek o problematice, zároveň měly být analyzovány současné přístupy k bezpečnosti kyberprostoru. Touto analýzou mělo být zjišťováno, nakolik jsou příslušné autority ovlivněny předsudky a stereotypy tradičního strategického přemýšlení, v jakých oblastech jsou si případy podobné a jaké mají apriorní předsudky či ustálené předpoklady charakteristické v této oblasti. Právě v tomto okamžiku při analýze politických dokumentů došlo k poznání, že cesta k cíli zřejmě tímto směrem nevede a je třeba se zaměřit více na samotnou podstatu uzlů. Případové studie kybernetických strategií nefungovaly, nepřinášely dostatečně zajímavá data, dostatečně charakterizující centrální

[15] DRULÁK, Petr. *Jak zkoumat politiku: kvalitativní metodologie v politologii a mezinárodních vztazích*. Praha: Portál, 2008. ISBN 978-80-7367-385-7. s. 20

uzly. Jejich klasifikace byla v teoriích buď velmi obecná či příliš konkrétní a postup práce proto nevedl k žádným smysluplným závěrům.

Například Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 mluví o kritické informační infrastruktuře (národní aktéři, KII, VIS)[16] či národních aktérech kybernetické obrany. Dále však s těmito aktéry není pracováno, nejsou analyzovány jejich specifika v národní kybernetické obraně a především jejich role v kyberprostoru, odhlédneme-li od pouhé bezpečnosti jich samotných. Jinými slovy není ve strategii kybernetické obrany definováno, jak oni sami přispívají k bezpečnosti kyberprostoru.

Dále je soukromý sektor a jeho uzly v kybernetické strategii ČR[17] popsán jen velice obecně, bez konkrétnějšího rozpracování. Uvedeny jsou záměry jako „*Vytvořit v kooperaci se soukromými subjekty jednotné bezpečnostní normy, standardizovat spolupráci a stanovit povinnou úroveň zabezpečení pro subjekty kritické informační infrastruktury.*“[18] či „*Zajistit v kooperaci se soukromým sektorem kyberprostor, poskytující spolehlivé prostředí pro sdílení informací, výzkum a vývoj a zajistit bezpečnou informační infrastrukturu stimulující podnikání soukromých subjektů v zájmu podpory konkurenceschopnosti všech podnikajících soukromých subjektů v České republice a chránicí jejich investice.*“[19] Z těchto prohlášení je velmi složité vytvořit závěr, jak se kybernetická strategie ČR staví k hlavním centrům a uzlům internetu.

Obdobně se k problematice staví také kybernetická strategie USA. Jako uzly jsou zde zpozorovatelné především prvky kritické infrastruktury a (obvykle na vládu navázaná) centra kybernetické obrany.[20]

---

[16] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-05-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

[17] Ibid. s. 19.

[18] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-05-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf. s. 19.

[19] Ibid. s. 19.

[20] *The National Strategy to Secure Cyberspace*. Morgan James Publishing, 2003. ISBN 9780976090144.

Práce v současné podobě ale navrhuje, aby pokud mluvíme o bezpečnosti v souvislosti s velkými uzly, například i těmi, popsanými v kybernetických strategiích (tedy kritické informační infrastruktuře, významných informačních systémech apod.), abychom je chápali šířeji, než jen jako bezpečnost uzlů samotných. Vzhledem k jejich významu, jsou centra jedni z hlavních aktérů bezpečnosti kyberprostoru, sami bezpečnost zajišťují, podílí se na ní a především – mohou ji ohrožovat.

Teorie a metodologie

Při změně zaměření práce na centra musela být změněna také metodologie práce. Ta stále operuje v rámci kvalitativního výzkumu a za účelem její koncentrace na činnost uzlů v kyberprostoru byla jako metoda zvolena jedinečná případová studie, a to její poddruh disciplinovaná interpretativní studie.[21] Ta se pohybuje na pomezí jedinečné a instrumentální studie.[22] Disciplinovaná interpretativní studie si vybírá za případ fenomén kyberprostoru vhodný pro svou jedinečnost a význam pro mezinárodní bezpečnost. K jeho zkoumání bude využita teorie sítí od A. L. Barabásiho, která dosud na daný fenomén tímto způsobem dle dostupných rešerší nebyla aplikována. Teorie však slouží pouze jako vodítko pro identifikování hlavních procesů a proměnných – především role uzlů a center v kyberprostoru a oblastí, v rámci kterých nabývají odlišných významů. Případ, tj. fenomén kyberprostoru „tedy neslouží jako nástroj pro práci s teorií, ale naopak teorie je vodítkem pro práci s případem."[23]

Práce také využívá holistické teorie při zkoumání sociálních struktur,[24] které v různé intenzitě vytváří společnost při využívání kyberprostoru pro vzájemnou interakci a komunikaci.

Jak bylo již zmíněno v úvodu, práce se ptá na otázky spojené s rolí centrálních uzlů a jejími dopady na kyberprostor jako na sociální prostředí.

---

[21] DRULÁK, Petr. *Jak zkoumat politiku: kvalitativní metodologie v politologii a mezinárodních vztazích*. Praha: Portál, 2008. ISBN 978-80-7367-385-7. s. 34
[22] Ibid. s. 34
[23] Ibid. s. 34
[24] Ibid. s. 23

Základní výzkumná otázka diplomové práce zní: **Jaké jsou možnosti zlepšení strategií pro kybernetickou bezpečnost aplikací Barabásiho teorie center na kyberprostor?**

Práce se nesnaží jednotlivé **náhledy** příliš strukturovat a rozmělňovat, neboť jak uvádí Barabási[25], redukcionismus, tedy snaha o zjednodušení, již nadále v oblasti reálných sítí nestačí. Jsou to velice komplexní světy a podrobná analýza některých jejich částí v kontextu reality může přinést zajímavá zjištění, která by jinak zůstala skryta. Během poslední dekády bylo postupně více a více sítí zkoumáno ve své komplexitě. Redukcionismus totiž dekonstruuje komplexní systém na pouhé uzly a jejich spojení. Teorie sítí nám pomáhá je znovu skládat do obrazu, jaký samy o sobě představují tak, abychom mohli vidět celkový obraz. To ovšem při vědomí, jaký význam centra a k nim natažené vazby mají. Barabási to nazývá zjevení skrytím. Tedy pokud skryjeme jednotlivé podrobnosti, které jsme již poznali, můžeme se více zaměřit na vyšší souvislosti. Je přesvědčen, že žádná teorie buněk, sociálních sítí nebo internetu dnes nemůže ignorovat jejich vzájemné propojení v síť, ani sítě samotné.[26]

Jelikož se práce věnuje kyberprostoru, budou v textu často používány termíny, které odpovídají jeho terminologii. Pojmy, které nemají oficiální české ekvivalenty, nebudou překládány, ale ponechány v anglické verzi. Zkratky, případně méně známé termíny budou vysvětleny v poznámkovém aparátu.

Zpracování práce bylo náročné, protože pohledy na kyberprostor se napříč autory výrazně liší, jde navíc o poměrně odborné téma s mnoha technickými návaznostmi. V neposlední řadě jde o nový, neustále se měnící, sociální prostor s přibývajícími aktéry i oblastmi využití.

---

[25] BARABÁSI, Albert-László. The network takeover. *Nature physics* [online]. 2012, (8), 14-16 [cit. 2016-05-10]. Dostupné z: http://www.mamartino.com/img/Barabasi_2012_The_network_takeover.pdf s. 14

[26] Ibid.

1. Teorie sítí dle A. L. Barabásiho

Albert Barabási[27] se před čtrnácti lety ve své knize zaměřil na zkoumání world wide web (www), celosvětové sítě, často zobecněné do pojmu internet. Zjistil, že www není zcela náhodná síť, nýbrž vykazuje znaky samoorganizace.

Jednou z myšlenek, které ho ke zkoumání sítí vedly, byla známá studie Stanley Milgrama z roku 1967,[28] jež tvrdí, že lidé jsou na světě propojeni sítí sociálních vazeb, která nám umožňuje znát v průměru přes šest uzlů všechny obyvatele planety. Vžilo se pro ni označení *šest kroků od sebe*. Inspirován touto studií provedl Barabási analýzu world wide webu a zjišťoval, kolika odkazy jsou v této síti od sebe v průměru vzdáleny uzly, tedy webové stránky. Dospěl k výsledku 19.[29] Tedy ke každé stránce www by se mělo z jiné stránky dostat v průměru přes 19 odkazů. To se může zdát jako velký rozdíl, ale ve skutečnosti při počtu uzlů a vazeb v takové síti je to vzdálenost minimální (sám Barabási ale upozorňuje, že je třeba toto číslo brát s rezervou. Výsledkem bylo zjištění, že sociální vazby mezi lidmi i uzly ve world wide webu jsou vlastně malé světy.

Tyto sítě nemají náhodně vytvářené vazby a počty vazeb se nepohybují v jedné škále – proto je nazýváme bezškálové. Pro zkoumání kyberprostoru jsou výhodné, protože mají několik specifických vlastností.

Sítěmi však v tomto případě nemusí být pouze internet, podobnou bezškálovost Barabási popisuje i v dalších odvětvích – v sociálních vazbách hollywoodského filmového průmyslu či vzdálenosti osobních vazeb mezi jednotlivými obyvateli planety. Dokonce i v biologii, například v síti buněčného metabolismu. Protože však Barabási zkoumal bezškálové sítě původně prostřednictvím internetu, nabízela se myšlenka tuto teorii v diplomové práci dále zkoumat a zjistit, jakou roli v něm uzly hrají. A protože internet, world wide web a obecně světové komunikační sítě mají hodně společného, lze tak obecně zkoumat roli uzlů v celém kyberprostoru.

---

27 BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3.
28 MILGRAM, Stanley. The Small World Problem. *Psychology Today*. **1967**(2), 60-67.
29 BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 31-45.

1.1 Malé světy

Malé světy, tedy relativní blízkost uzlů přes několik prostředníků, dovedly Barabásiho k myšlence, že jsou to právě centra, uzly s velkým počtem vazeb na ostatní, která umožňují být dvěma uzlům nedaleko od sebe. Že právě centra zkracují tuto vzdálenost. Ale jak ona centra vznikají? Proč se zrovna jim podařilo získat tolik vazeb a jaký vzorec stojí za jejich fungováním? Tyto otázky vedly ke zjištění, že uvnitř www, stejně jako uvnitř sociálních skupin ve společnosti, dochází ke zvláštní formě samoorganizace. Matematickým zkoumáním zjistil, že se v těchto sítích nevyskytuje klasická Gaussova sociologická křivka. Nelze v nich nalézt škálu či typického zástupce uzlu. Vyskytuje se v něm ovšem vždy určité množství center, která mají na sebe navázáno mnohem více uzlů, než ostatní, tedy že mají mnohem větší konektivitu. Rozhodl se proto zkoumat rozdělení konektivity mezi uzly v síti a zjistil, že se řídí mocninným zákonem.

„Příkladem mocninných zákonů je […] třeba průměrná doba trvání jednoho biologického druhu. Na jeden druh žijící řekněme 100 milionů let připadají dva druhy trvající 50 milionů let, 10 druhů trvajících 10 milionů let atd. Existuje jen velmi málo druhů, které přežívají dosti dlouho, a velmi mnoho druhů, které žijí jen krátce. Kdyby se stejně řídila výška lidí, pak by (např.) všude kolem nás chodili lidé vysocí […] metr padesát, zatímco občas bychom naopak narazili na člověka vysokého pět metrů.“[30] Mocninný zákon umožňuje vznik většího množství center.

Otázkou je, proč se zrovna www řídí mocninným zákonem? Jaká síla jej nutí, aby se takto sám vnitřně organizoval? Odpovědí je přítomnost dvou zákonů: růstu a preferenčního připojování.[31] Obě podmínky jsou nutné a pro ideální model bezškálových sítí také samy o sobě dostatečné. Znamenají, že aby se síť mohla stát bezškálovou, musí stále růst. Stále musí přibývat nové uzly a nové vazby. Preferenční připojování pak znamená, že nově vznikající vazby nejsou náhodné, nýbrž se připojují podle vlastního vnitřního klíče. Tím klíčem je jednak **velikost** uzlu (a tedy i jeho stáří, neboť při neustálém růstu sítě mají starší uzly výhodu ve velikosti) a jednak jeho **zdatnost**. Zdatnost, nebo

[30] HOUSER, Pavel. Mocninné versus normální zákony – a co z toho vyplývá. In: *Scienceworld* [online]. [cit. 2016-05-13]. Dostupné z: http://www.scienceworld.cz/neziva-priroda/mocninne-versus-normalni-zakony-a-co-z-toho-vyplyva-1716/
[31] Ibid. s. 89.

také atraktivita, udává, jak velkou budou mít ostatní uzly tendenci připojovat se k danému centru. Tato zdatnost vysvětluje, proč dnešní největší centra nejsou zároveň těmi nejstaršími. Zdatnost jednotlivých uzlů je velmi důležitá a ovlivňuje ji komplex faktorů. Barabási jev vystihuje spojením „bohatí bohatnou a chudí chudnou“.[32] Tento princip může dle teorie za vznik velkých center ve www.

1.2 Topologie sítí

Barabási vytvořil topologii *bezškálové* sítě a postavil ji vedle dvou dalších modelů sítí – hierarchické a rozptýlené. *Hierarchická* se dá připodobnit k pyramidě a lze ji nalézt u liniového řízení například v armádě nebo v managementu soukromých společností. Vyznačuje se zejména navázáním téměř všech uzlů na jedno řídící centrum, které stojí na vrcholu pyramidy. Síť je proto velmi závislá na tomto hlavní centru a silně centralizovaná. Velmi názorně je tato typologie uvedena v Příloze 1.

Rozptýlená síť naproti tomu vůbec netvoří centra, tedy uzly s vyšším počtem vazeb než mají ostatní. Připomíná tak například silniční síť bez dálnic. Mezi její výhody patří obrovská robustnost, jež je rovněž důležitá vlastnost sítí[33] a u jednotlivých druhů se liší. Robustnost u rozptýlené sítě je velmi vysoká, neboť každý uzel lze jednoduše obejít po velmi krátké objížďce, a tak nemá ztráta daného uzlu na funkčnost sítě velký vliv. Analogii lze nalézt například také u tkalcovské osnovy nazývané rip-stop. I přes poškození látky na mnoha místech drží síť díky pravidelným uzlům a vazbám stále pohromadě. Topologie rozptýlené sítě byla původně plánovaná i u internetu. Ten se však začal rychle rozšiřovat a organicky přešel do bezškálové struktury.

Zajímavým poznatkem je, že ač se obecně soudí, že Al-Káida byla síť tvořená jednotlivými buňkami[34] a měla by tak být vlastně síť rozptýlená, dle Barabásiho zjištění

---

[32] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 83.
33 Ibid. s. 111.
[34] Např. ATWAN, Abdel Bari. *The Secret History of al Qaeda*. London: Saqi, 2012. ISBN 9780863568435.

i její topologie odpovídala bezškálové síti. Tato teroristická organizace tedy byla rovněž decentralizovanou sítí ve výše popsaném pojetí.[35]

Jak popisuje Barabási, topologická *robustnost* je strukturální součástí reálných sítí. Je to vlastnost vycházející přímo ze samé podstaty sítě a její organizace a zásadním způsobem se na ní podílejí právě centra. Ta poskytují síti stabilitu a díky nim náhodné odebírání uzlů pro síť nepředstavuje vážné riziko. Při náhodném poškozování uzlů je totiž málo pravděpodobné, že bude ohrožen právě velký centrální uzel. Barabási tím ukazuje, že topologická robustnost bezškálových sítí je velmi vysoká (ač nedosahuje robustnosti sítě rozptýlené), neboť abychom síť zničily, je třeba odebrat většinu center. Dle Barabásiho výzkumu je hlavním hrozbou pro takovou síť poškození jejích největších uzlů. Avšak ani odebrání několika centrálních uzlů ještě nezpůsobí selhání sítě. Teprve po zániku většiny center se začne síť rozpadat a fragmentovat na malé ostrůvky. Z toho vyplývá, že pokud se má daná síť narušit, je třeba se při útoku **zaměřovat na centra**.[36]

1.3 Centra

Nejdůležitější částí této teorie je tedy *přítomnost center*. Centra a jejich role je klíčová pro jakoukoli bezškálovou síť a stejně tak pro kyberprostor. Centra ovlivňují strukturální stabilitu reálných sítí, jejich dynamické chování, robustnost a odolnost vůči chybám a útokům zvnějšku. Jsou důkazem vysoce důležitých organizačních principů, které řídí evoluci sítí.[37]

Z výše uvedeného můžeme odvodit jednotlivé **vlastnosti centrálních uzlů**:

1) Díky centrům je možné na kyberprostor nahlížet také jako na sociální prostor, ve kterém silné uzly **ovlivňují chování** těch slabších (ač jde jistě i o ovlivňování vzájemné).

2) Centra **zkracují vzdálenost** mezi jednotlivými uzly, neboť díky velkému počtu vazeb se může komunikace mezi dvěma obyčejnými uzly odehrát

[35] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 212.
[36] BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3. s. 116.
[37] Ibid. s. 75.

prostřednictvím centra a není třeba uskutečnit tolik kroků, tj. navštívit po cestě tolik uzlů.

3) Centra mají také schopnost **akumulovat uzly**, jsou pro ně totiž atraktivní (mají vysokou zdatnost), a proto uzly preferují vytváření vazeb na ně a ne na nějaké jiné menší uzly. Tím centrům ještě více **roste atraktivita** a lákají další nové uzly.

4) Přes centra rovněž **prochází velká část komunikace v síti**, protože tím, že zkracují cestu, většina informací (mluvíme-li například o kyberprostoru) je při své cestě navštíví, aby si cestu zkrátila.

5) V žádné jiné oblasti lidské interakce zřejmě není význam uzlů tak dominantní, jako právě v kyberprostoru. Tím, že komunikační technologie bezprecedentně urychlují všechny procesy v síti (tj. kyberprostoru), všechny vlastnosti této bezškálové sítě se **umocňují**.[38]

6) V neposlední řadě jsou centra také **pilíře sítě**, na kterých síť stojí a po jejichž odstranění se může rozpadnout.

Že je centra nutné chránit není samo o sobě objevné zjištění. Autoři, kteří psali strategie kybernetické bezpečnosti, si tohoto ohrožení byli vědomi i bez aplikace Barabásiho objevu. Logicky je napadlo, že tato centra jsou hodna ochrany[39] a často je pod různými pojmy do těchto strategií zahrnovali (např. kritická informační infrastruktura, významné informační systémy[40]).

---

[38] Srovnejme například kyberprostor s Barabásiho oblíbenou skupinou herců v Hollywoodu. Sebeznámější herec s maximem vazeb (známostí) na ostatní nedosahuje ani zlomku sociálního postavení, jaké mají velké uzly v kyberprostoru. Ať už je chápeme jako NSA, Facebook nebo Google. Množství vazeb, které se kolem nich každou vteřinu vytváří, je enormní. V každý moment přes tyto uzly proudí obrovské množství informací, které tyto centra v každém okamžiku využívají. Všechny dosavadní lidské sociální sítě a skupiny před příchodem kyberprostoru se s ním nemohou vůbec poměřovat. I z toho je možné dovozovat, že centra v tomto prostředí získávají velkou moc.

[39] *The National Strategy to Secure Cyberspace*. Morgan James Publishing, 2003. ISBN 9780976090144.

[40] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-05-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

Kyberprostor splňuje první z podmínek bezškálové sítě a to, že stále roste. Rozvinutím výše popsaných vlastností můžeme dovodit, že centrům se zvyšujícím se počtem vazeb také *neustále roste vliv*. Síť se tím více centralizuje, přibližuje se k hierarchické topologii sítě a centra se stávají hybatelem kyberprostoru. Ten, kdo má nad těmito uzly kontrolu a dokáže je ovládat, je sám velmi *vlivný hybatel* v kyberprostoru a může využívat všechny vlastnosti popsané výše. A pokud přijmeme předpoklad, že kyberprostor je důležitou oblastí národních zájmů státu, pak by se stát měl zabývat tím, kdo je tím vlivným hybatelem a zda jím nemá být v případě některých center on sám.

Thomas Rid ve svých výzkumech dokazuje, že kybernetických útoků **přibývá**, ale jsou **méně hrozivé**.[41] Pokud se na tento jev podíváme optikou teorie sítí, lze to vysvětlit právě vzrůstajícím počtem uzlů, které vedou k nárůstu počtu útočníků, ale rovněž vzrůstající silou center, což naopak snižuje jejich zranitelnost. Centra se s přibývajícími vazbami stávají důležitější, a proto jsou více a více chráněna. Možnost poškodit centrum nebo dokonce část sítě je v dnešní době již velmi malá. Kybernetická válka cílená tímto směrem proto nedává smysl.[42]

Co jsou centra v praktickém významu kyberprostoru? Zde záleží, jak na něj nahlížíme. Tj. s jakým náhledem k němu přistupujeme, **jaké účastníky** kyberprostoru vnímáme jako uzly samotné. Z nich pak lze identifikovat i centra, tedy uzly s největším počtem vazeb.

Ač je kyberprostor ve své ideální podobě bezškálová síť, stále se jedná o síť vytvořenou člověkem. Jde v ní proto najít mnoho odlišností od ideálního modelu bezškálové sítě. Tou hlavní odlišností je jeho uměle vytvořená struktura, kterou je možné cíleně měnit. Například tvorbou nových vazeb či uzlů, jejich přeorientováváním či zvyšováním zdatnosti (atraktivity) jednotlivých uzlů. A především změnou technologie.

---

[41] RID, Thomas. *More Attacks, Less Violence*. Journal of Strategic Studies [online]. 2013, vol. 36, no. 1, pp. 139-142. ISSN 0140-2390.
[42] RID, Thomas. *Cyber war will not take place*. New York: Oxford University Press, 2013. ISBN 9780199330638.

2. Konceptualizace kyberprostoru

Práce nepatří do oborů přírodovědných, nýbrž sociologických, a proto je třeba právě skrze pohled bezpečnostních studií kyberprostor konceptualizovat.

Kyberprostor je napříč odbornou literaturou nahlížen různě. Můžeme o něm říci, že neexistuje v jedné propojené entitě, ale v různých paralelách. Nelze jej proto jednoduše "ovládnout", avšak lze ovládnout některé paralely.[43] Proto hovoříme o kyberprostoru v náhledech, které jsou vždy ohraničeny rolí jednotlivých uzlů a záleží na subjektivním pohledu pozorovatele, co vše do něj zahrne. Přesné vymezení je velmi složité. Proto i v této práci jsou jednotlivé náhledy jen nastíněny, aby posloužili jako rámec pro aplikaci teorie. Podle Libického by měl být pojem kyberprostor užíván s rozvahou a neuváděn tam, kde by mohl být vnímán jako ohraničená doména.[44]

2.1 Vojenský pohled na kyberprostor

Tradiční vojenský přístup ke kyberprostoru zastoupený například americkým ministerstvem obrany[45] chápe kyberprostor jako další doménu, vedle pozemního, námořního, leteckého a vesmírného boje, která umožňuje použít na její operacionalizaci stávající vojenské strategie, jako je například strategie odstrašení, či nutnosti „zřídit, vyškolit a vybavit“ [46] jednotky určené k boji v kyberprostoru. Ten jako novou doménu uvádí např. také Lynn III.[47] Vojenský přístup používá pojmy jako kybernetická válka či

[43] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 326
[44] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 335
[45] *The National Strategy to Secure Cyberspace*. Morgan James Publishing, 2003. ISBN 9780976090144.
[46] Department of Defense Strategy for Operating in Cyberspace. *Computer Security Resource Center (CSRC)* [online]. [cit. 2016-05-13]. Dostupné z: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
[47] LYNN III, W. J. 2010. Defending a New Domain: [Essay]. Foreign Affairs, 97-108. poh, EBSCOhost. Retrieved from: http://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=52957873&site=ehost-live

kybernetická nadvláda (*superiority*).[48] Tento pohled je v literatuře značně zpochybňován, protože vede například ke zveličování kybernetických hrozeb a k tendenci sekuritizovat i témata, kterým tento přístup škodí.[49] Je však třeba vnímat důvod, proč k tomuto dělení Ministerstvo obrany USA přistoupilo – bylo třeba jednoznačně vymezit kyberprostor jako oblast, jež má svá nevyvratitelná specifika, a jako takovou na ni alokovat zdroje, a také pozornost občanů a politiků. Částečně díky tomuto diskurzu začali političtí představitelé vnímat vojenský potenciál kyberprostoru na úrovni rovnocenné s ostatními prioritami obranných strategií.

Tato vojenská perspektiva používá stejnou logiku, jako strategie vyvinuté během studené války, avšak pro odlišné oblasti. Útoky v Estonsku v roce 2007[50] vedly k tomu, že je někteří začaly vnímat jako nový druh války. Proto k ní bylo přistupováno pohledem válečných strategií, například strategií odstrašení. Ač platné globální dohody týkající se bezpečnosti kyberprostoru mohou mít určitý odstrašující efekt na vojenské či špionážní úrovni, vzhledem k **problému přisouzení**[51] nemusí být jejich dopad tak velký jako v případě jaderných nebo konvenčních zbraní. To je viditelné u nestátních aktérů

[48] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 328

[49] SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie (Defence and Strategy)* [online]. 2014-7-15, **14**(1), 29-38 [cit. 2016-05-13]. DOI: 10.3849/1802-7199.14.2014.01.029-038. ISSN 12146463. Dostupné z: http://www.defenceandstrategy.eu/cs/aktualni-cislo-1-2014/clanky/critical-comments-on-current-research-agenda-in-cyber-security.html#.U7ZXZ1OAI_0. s. 29

[50] Kybernetické útoky Ruska na servery v Estonsku - CZOSSECK, Christian, Rain OTTIS a Anna-Maria TALIHARM. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. *Cooperative Cyber Defense Center of Excellence Website* [online]. 2011 [cit. 2016-05-13]. Dostupné z: https://www.researchgate.net/publication/220143696_Estonia_after_the_2007_Cyber_Attacks_Legal_Strategic_and_Organisational_Changes_in_Cyber_Security

[51] Problém přisouzení vyplývá ze samotné architektury kyberprostoru jako decentralizované sítě. „Bezpečností tehdy byla vůle síť maximálně decentralizovat a tím zajistit její funkčnost i v případě jaderného útoku. Paradoxně právě toto technologické řešení zajistilo pro dnešní hackery de facto absolutní anonymitu, pokud neudělají flagrantní chybu.“ v BUREŠ, Oldřich (ed.). *Bezpečnost v době neklidu: sborník vybraných příspěvků ze studentské konference pořádané v Brně 19. dubna 2013 Centrem bezpečnostních studií Metropolitní univerzity Praha, Centrem pro bezpečnostní a strategická studia a Oddělením pro Bezpečnostní a strategická studia Fakulty sociálních studií Masarykovy univerzity v Brně* [online]. Praha: Metropolitan University Prague Press, 2013 [cit. 2016-07-28]. ISBN 978-80-86855-92-9. s. 83

(hackerů, teroristů, zločinců či nespokojených občanů), na něž mají tyto normy jen malý efekt.[52]

U některých autorů se objevuje snaha vyvinout strategii, obsahující v sobě vybudování takových kapacit, aby bylo možné potenciálního útočníka odradit od jeho úmyslu útočit.[53] Pravdou je, že stejný útok, jaký byl spáchán na Estonsko, by dnes již nebyl možný. Kyberprostor je neustále se vyvíjející (fluidní) prostředí, kde nelze brát momentální hrozby jako výchozí stav pro konflikty v budoucnu. Problém nedostatečné obrany Estonska byl proto jednoduše vyřešen **technickými opatřeními**.[54] Nabízí se úvaha, kolik jednotlivých hrozeb, ukrytých v kyberprostoru, bude možné nakonec vyřešit technickými opatřeními? Nebude to nakonec většina?

Nejen technickými opatřeními lze kyberprostor měnit. Stevens[55] pojednává o možnosti odstrašení protivníka v kyberprostoru a o legislativních normách, jež by tuto strategii umožnily. Naráží při tom na důležitý fakt, že kyberprostor, jakožto uměle vytvořenou doménu je možno **normami tvarovat** do stavu příhodného pro stát.[56] Upozorňuje tím na fakt, že prostřednictvím norem je možné nastavit pravidla chování sítě, jednotlivých uzlů a mantinely, uvnitř kterých budou fungovat.

---

[52] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 163

[53] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 149

[54] SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie (Defence and Strategy)* [online]. 2014-7-15, **14**(1), 29-38 [cit. 2016-05-13]. DOI: 10.3849/1802-7199.14.2014.01.029-038. ISSN 12146463. Dostupné z: http://www.defenceandstrategy.eu/cs/aktualni-cislo-1-2014/clanky/critical-comments-on-current-research-agenda-in-cyber-security.html#.U7ZXZ1OAI_0. s. 29

[55] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 159

[56] LIBICKI, Martin C. *Conquest in cyberspace: national security and information warfare*. New York: Cambridge University Press, 2007. ISBN 978-0-521-69214-4. s. 31–37.

Užitečnou cestu ve vojenském paradigmatu nabízí příručka pro informační operace,[57] která rozděluje kyberprostor na tři propojené oblasti: 1) systémy konektivity, 2) obsah či informaci, která může být v kterýkoli čas okamžitě poslána kyberprostorem a 3) lidské rozpoznání této informace s následnou reakcí a rozhodnutím. Toto rozdělení[58] totiž poměrně dobře ilustruje **lidský prvek**, který je v kyberprostoru velice podstatný.

Zajímavý pohled na boj v kybernetickém prostoru představuje článek od střediska CESES,[59] který vnímá boj v kyberprostoru jako formu neletální, tedy nesmrtící zbraně, která má požadovaný účinek – vyřadí z provozu zamýšlená zařízení, ale nutně u toho nezabíjí zúčastněné osoby. Sabotáže, špionáž, psychologické operace, propaganda jsou formy útoků v kyberprostoru zdaleka nejčastější. Boj v kyberprostoru proto spíš než konvenční připomíná **asymetrický konflikt**. Již autoři Arquilla a Ronfeld[60] v roce 1996 argumentovali, že kybernetická válka bude spíš podobná konfliktům nízké intenzity, ve kterých má jasnou výhodu agresor. Možnost odstrašení se v kyberprostoru potýká s mnoha problémy, a proto se podle nich vrací tradiční pohled na boj, platný před existencí jaderných zbraní, který staví na principu akce a reakce mezi útokem a následnou obranou. Rovněž podle Stevense, vedou nestátní aktéři v kyberprostoru spíše guerillovou válku (zajímavým přirovnáním je i kybernetické vandalství), u které odstrašení příliš nefunguje. I kdyby bylo možné využít kybernetické odstrašení mezi státy, problém nastane při jeho uplatnění vůči **nestátním aktérům**, kteří mají na rozdíl od konvenčních těžkých zbraní, většinu nástrojů pro boj v kyberprostoru dostupnější.[61]

---

[57] SCAPARROTTI, Curtis. *Joint Publication 3-13 Information Operations* [online]. In: Joint Publication. 2012 [cit. 2016-05-12]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

[58] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 72

[59] BALABÁN, Miloš, Antonín RAŠEK a Martin POTŮČEK. Rodící se nová ohrožení v neklidném světě. *Vojenské rozhledy* [online]. 2011, **20**(4), 3-21 [cit. 2016-05-10]. ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/rodici-se-nova-ohrozeni-v-neklidnem-svete

[60] ARQUILLA, John. a David F. RONFELDT. *The advent of netwar* [online]. Santa Monica, CA: RAND, 1996 [cit. 2016-07-28]. ISBN 08-330-2414-0. Dostupné z: http://www.rand.org/pubs/monograph_reports/MR789.html p. 94.

[61] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 164

Podle kritiků tohoto přístupu, není zkoumání hrozeb vojenskou perspektivou založené na kritické analýze dopadů kybernetického útoku, rozvoje technologií nebo možných opatření, nýbrž na přemýšlení o tom, co se může stát.[62]

Na opačnou stranu konceptualizace kyberprostoru a jeho vnímání jako specifického sociálního prostředí se staví mnoho autorů. Libicki například myšlenku páté domény odmítá mimo jiné proto, že všechny útoky v kyberprostoru jsou možné **jen skrze zranitelnosti** jednotlivých prvků. To nelze říct například o hrozbě útoku jadernou zbraní na města. Hlavním důvodem tedy není kyberprostor tvořený lidmi (to jsou i ona města), nýbrž schopnost obránců jej měnit.[63] Opět tím poukazuje na jeho proměnlivost. Obdobně tento názor odmítá Schmitt[64] a argumentuje především problémy při analogickém uplatňování mezinárodního (vojenského) práva na novou doménu. Obdobně Schmidt upozorňuje, že zacházení s kyberprostorem stejně jako s prostředím pozemním, mořským či vzdušným, není vhodným uchopení definice kyberprostoru, neboť tato doména podle Schmidta neexistuje ve formě čtyř zbývajících. Ty totiž existují zcela reálně a člověk, aby je ovládl, se jim musí přizpůsobit. Kyberprostor je jiný. Není třeba se mu přizpůsobovat, protože je možné prostě a jednoduše přizpůsobit přímo jej. Proměnlivost se opět ukazuje jako velmi důležitá.

Je třeba nezaměřovat se na kyberprostor jako na fyzický prostor. Schmidt toto pojmenovává jako epistemologickou chybu výzkumníků, kteří se snaží problém

---

[62] SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie (Defence and Strategy)* [online]. 2014-7-15, **14**(1), 29-38 [cit. 2016-05-13]. DOI: 10.3849/1802-7199.14.2014.01.029-038. ISSN 12146463. Dostupné z: http://www.defenceandstrategy.eu/cs/aktualni-cislo-1-2014/clanky/critical-comments-on-current-research-agenda-in-cyber-security.html#.U7ZXZ1OAI_0

[63] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 323-324

[64] SCHMITT, M. N. 2012, „International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.“ Harv. Int'l L.J. Online, vol. 54, no. 13.

zjednodušovat bez snahy vytvořit teoretický základ, který by poskytl adekvátní pohled na kyberprostor a hrozby, které přináší.[65]

Schmidt zcela nevylučuje použití kyberprostoru k velkým útokům, upozorňuje však na vzájemnou propojenost, a tedy škodu způsobenou potenciálně oběma stranám konfliktu. Samotný útok bude spíše **dobře připravenou sabotáží**, se snahou zakrýt původce akce, než otevřený útok na nepřítele. Ostatně budování nákladné obrany před ničivým, ale málo pravděpodobným útokem nedává moc velký smysl ani politicky, ani strategicky.[66]

Mueller poznamenává, že každodenní obrana proti kybernetickým hrozbám spočívající v **identifikaci, prevenci a reakci** na hrozby vytváří mezinárodní síť kontaktů, která spoléhá na vzájemnou spolupráci a normy vytvořené státy a postupně zvyšuje bezpečnost zapojených aktérů.[67]

Schmidt proto poukazuje na potřebu přistupovat ke kybernetické bezpečnosti nejen z pohledu totální války, ale z pohledu jeho běžného **každodenního fungování**. Z něj vyplývají spíše jiné formy ohrožení, než totální válka, a proto je na čase změnit náhled na kyberprostor optikou studené války a jaderného odstrašení. Měli bychom očekávat spíše snahy o ovlivňování politiky sousedního státu prostřednictvím **méně výrazných nástrojů** v kyberprostoru, než jsou kybernetické útoky s katastrofálními dopady.[68] Velmi sofistikovaná špionáž, rozvracení státu či kybernetické sabotáže jsou naopak velmi pravděpodobné a jsme jich již dávno svědky.[69] Jedním z nich, jak bude dále popsáno, je také **kontrola nad centry**.

---

[65] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 72.
[66] CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. In: *4th International Conference on Cyber Confl ict*. Talin: NATO CCD COE Publications, 2012, s. 141-153.
[67] MUELLER, Milton L. *Networks and States: The Global Politics of Internet Governance*. 1. Cambridge: The MIT Press, 2010 [cit. 2016-07-28]. ISBN 9780262290135. p. 164.
[68] CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. In: *4th International Conference on Cyber Confl ict*. Talin: NATO CCD COE Publications, 2012, s. 141-153.
[69] SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie (Defence and Strategy)* [online]. 2014-7-15, **14**(1), 29-38 [cit. 2016-05-13]. DOI: 10.3849/1802-

2.2 Kyberprostor pohledem sociálního konstruktivismu

Luke[70] navrhuje jiný koncept, kdy je kyberprostor vnímán jako **sociální struktura**, kde vznikají noví aktéři a organizace. Ačkoli můžeme tuto strukturu chápat jako prostor, jeho podoba je tvořená komunikačními uzly a jejich vazbami.

Samotné uvažování o kyberprostoru je v práci částečně ovlivněno jeho vymezením v práci Schmidta,[71] který staví kyberprostor na základy teorie sociálního konstruktivismu, a tak přistupuje k dříve technickému vnímání kyberprostoru jiným sociologicko-politologickým paradigmatem. Vybírá přitom práci sociologa Bruno Latoura,[72] který klasický sociální konstruktivismus doplňuje o přínos technologií v konstrukci naší sociální reality.

Uzly můžeme vnímat jako součást sociálního konstruktu. Vznikají jako výsledky lidského chování, lidských přání, lidské volby. Tím, jak lidé preferují jedny uzly před druhými na základě jejich zdatnosti, **vytvářejí realitu** kyberprostoru. Při každé volbě, kterou při výběru uzlu činí (a který tak podpoří), se jim naskýtá možnost skutečně vytvářet nový sociální prostor.

Sociální konstruktivismus je v kyberprostoru tvořen opakovanou činností aktérů – uživatelů, čímž vytváří institucionalizovaný konstrukt. Ty však samotným vytvořením svou činnost nekončí, naopak zpětně ovlivňují své uživatele, kteří přijímají návyky konstruktem očekávané. Každý uživatel tak koná skrze konstrukt to, co se od něj očekává,

---

7199.14.2014.01.029-038. ISSN 12146463. Dostupné z: http://www.defenceandstrategy.eu/cs/aktualni-cislo-1-2014/clanky/critical-comments-on-current-research-agenda-in-cyber-security.html#.U7ZXZ1OAI_0

[70] LUKE, Timothy W. Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace. *Spaces of Culture: City, Nation, World* [online]. 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 1999, s. 27 [cit. 2016-05-11]. DOI: 10.4135/9781446218723.n2. ISBN 9780761961222. Dostupné z: http://sk.sagepub.com/books/spaces-of-culture/n2.xml

[71] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 73

[72] LATOUR, Bruno. *Aramis, or, The love of technology*. Cambridge, Mass.: Harvard University Press, 1996. ISBN 0674043235.

co od něj očekávají další uživatelé. Tato nechtěná sociální kontrola vytváří vlastně kulturní chování.[73]

Pokud jsme již vyzkoušeli dosažení nějakého cíle daným způsobem, máme tendenci vyhýbat se alternativám, a naopak preferovat tuto v našich očích jistější cestu, i kdyby neznámá byla kratší. Tím se vytváří kognitivní vrstva našeho chování, což vede k udržování vazeb, které jsme již získali, a tedy k udržování daných uzlů na výsluní mezi centry. Kdybychom při každém připojení na internet hledali nový vyhledávač, těžko by mohl být Google tak masivním centrem. Udržováním naší kognitivní vrstvy a opakováním stále stejného chování udržujeme poměrně stálé vazby i v tak proměnlivém prostředí jakým je kyberprostor. Ten proto není jen o infrastruktuře, systémech či obsahu. Je tvořen především tak, že jej **stále dokola používáme a tím tvarujeme**.[74] Čas od času dojde ke změně našeho chování. Na doporučení kamaráda třeba přejdeme na jinou službu. Objeví se například jiné centrum s vyšší zdatností. Tedy uzel, ke kterému má pro nás větší smysl si vytvořit vazbu.

Schmidt tak ve své práci relativizuje[75] kyberprostor jako místo se svými vlastními neměnnými zákony. Naopak poukazuje na to, že kyberprostor, jako dílo člověka, se kontinuálně **vyvíjí vzájemnou interakcí** milionů aktérů, zvláště těch, které mají na změně vlastní zájem, a tedy vývoj ovlivňují. Zákony kyberprostoru si tak vytváříme my sami a world wide web pro svou neohraničitelnost a komplexnost neustále sám sebe mění přímo tím, jak ho používáme a jak se vyvíjí technologie. Schmidt doslova píše „struktura a její využívání jsou konstruovány ruku v ruce.“[76]

---

[73] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 73
[74] Ibid. s. 73.
[75] Ibid. s. 73
[76] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 75 (Překlad autora)

Kyberprostor je tak vlastně rozšířením naší běžné reality. I zde, jak uvádí Schmidt,[77] bychom mohli identifikovat sociální skupiny sídlící na nějakém území a hovořící stejným jazykem. Kyberprostor však těmto skupinám umožnil identifikovat se na základě subjektivnějších znaků, než je řeč a místo bydliště. Národní státy se obávají, že by mohly nad těmito novými územími **ztratit vliv**. Můžeme nalézt mnoho příkladů, jak sociální struktury v kyberprostoru přesahují legislativní rámec států.[78] Jsou to ale opět **centra**, prostřednictvím kterých může stát svůj vliv realizovat.

2.3 Proměnlivost kyberprostoru

V práci byla již několikrát zmíněna důležitá vlastnost kyberprostoru, a to jeho proměnlivost.[79] Běžné sociální struktury totiž v čase tvoří stabilní konstrukty, které však kvůli proměnlivosti nejsou v kyberprostoru tak pevné,[80] a proto má tento sociální prostor větší **tendenci ke změnám**. Například před příchodem kyberprostoru se téměř každá sociální vlna ve společnosti nějak zakotvila, ať to byly náboženské vlny ve starověku a středověku, nebo hudební vlny ve dvacátém století. A byť některé po letech odešly, obvykle přežily dekády a často své kořeny ve společnosti stále mají. Oproti tomu módní či virální vlny v kyberprostoru mizí velice rychle a málokteré se podaří výrazněji zasáhnout do dějin kyberprostoru a zanechat v něm více, než jen svou stopu.

Proměnlivost je, jak víme již od Barabásiho, součástí všech bezškálových sítí. Ideální model bezškálové sítě však stále roste, vznikají nové a nové uzly a vazby. V reálných sítích však tyto vazby a uzly i zanikají. Vznikají a mizí také centra. Tento fakt je prvním, který tato práce vyjmenovává, a jež by se měl projevit i v kybernetické strategii daného státu. I když totiž vymezí svůj obecný postoj k centrům a vyjasní přístup k těm konkrétním, měl by počítat s tím, že může s určitou pravděpodobností některé **centrum zaniknout**.

---

[77] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 75
[78] Ibid. s. 76
[79] Ibid. s. 74
[80] Ibid. s. 74

2.4 Definice a typologie kyberprostoru

Pro práci se zdá nejvhodnější definice používající politologický model vnímání kyberprostoru, na rozdíl od definic vnímajících kyberprostor jako soubor mnoha technologických jednotek.[81] Práce proto přistupuje na vymezení, jež ve své práci používá i Schmidt,[82] který výstižně vybírá slova Daniela Kuehla: „Kyberprostor je doména, jejíž výjimečný […] charakter rámují elektronické […] nástroje určené k vytváření, ukládání, pozměňování, vyměňování a využívání informací prostřednictvím propojených systémů informačních a komunikačních technologií a na ně navazující infrastruktury."[83]

Martin Libicki rozeznává čtyři úrovně kyberprostoru[84] a zabývá se také možnostmi a prostředky, jak jednotlivé vrstvy poškodit. **První úroveň** je fyzická infrastruktura, hardware, vedení, směrovače, satelity apod. Lze je vyřadit fyzicky; zničením infrastruktury. **Druhou úrovní** jsou pravidla a principy, na který tento systém pracuje, jako jsou komunikační protokoly. Je možné je ovládnout převzetím zapojených systémů, například prostřednictvím malware. **Třetí** představuje pohyb dat – ať již těch uložených, či zrovna proudících. Narušení této vrstvy je možné například podvržením mailové komunikace či informací pohybujících se mezi směrovači. A nakonec **čtvrtá vrstva** je kognitivní, se kterou bude pracovat tento text převážně. K ní Libicki žádný způsob ovládnutí neuvádí, avšak jedna možnost se zdá být nasnadě. Právě skrze uzly a jejich velký vliv na kyberprostor.[85]

---

[81] Například DENNING, Dorothy Elizabeth Robling. *Information warfare and security*. Reading, Ma.: Addison-Wesley, c1999. ISBN 02-014-3303-6.
[82] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 71.
[83] KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. In: *Cyberpower and National Security*. Washington D.C.: National Defense University Press, 2009, s. 24-42. (Překlad autora)
[84] LIBICKI, Martin C. *Conquest in cyberspace: national security and information warfare*. New York: Cambridge University Press, 2007. ISBN 978-0-521-69214-4. s. 231-240.
[85] SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3. s. 71.

2.5 Náhledy na kyberprostor

Co znamenají centrální uzly v kyberprostoru, se liší podle toho, jak na kyberprostor **nahlížíme**. Libického první vrstva obsahující technické prvky bude zcela jistě zahrnovat centrální uzly, tvořené hlavními středisky technické sítě, stejně jako hlavní optické kabely a datová centra. Všechny tyto uzly budou mít jedno společné a to je jejich fyzická podstata. Jde o reálná zařízení umístěná v konkrétním státě a přístupná vymezenému okruhu osob.

Pokud opustíme takové rozdělení, můžeme si představit náhled, kde jednotlivé uzly tvoří **domény internetu** a ty nejnavštěvovanější v něm budou centry. Jiný náhled bude spočívat v množině kyberprostoru sestávající z **jednotlivých ISP**,[86] u něhož budou centry logicky ti největší poskytovatelé internetu. Jiným náhledem budou **technologické firmy** (jejichž zařazení jako součást kyberprostoru může být zpochybněno). Bezpochyby sem patří například společnost Apple, jejíž vliv, jakožto jednoho z centrálních uzlů kyberprostoru, je očividný. A takto bychom mohli pokračovat. Smyslem není přesně definovat jednotlivé náhledy, ale poskytnout čtenáři vysvětlení, co je pod pojmem **náhled** myšleno. V jednotlivých úvahách se proto mohou náhledy lišit a je mimo rozsah práce je přesněji vymezovat.

[86] Internet service provider – poskytovatel internetového připojení

3. Role státu v kyberprostoru

Ve třetí kapitole tato práce konceptualizuje roli státu v kyberprostoru a klade otázky, na kolik je **legitimní**, aby stát zasahoval do fungování kyberprostoru? Do jaké míry se hodlá **vměšovat** do kyberprostoru a kde jsou jeho **hranice**, za které již nepůjde? A pokud hodlá zasahovat, tak **jakými prostředky**? Jedním z nich je totiž jistě národní strategie kybernetické bezpečnosti.

Kde má stát hranice kontroly nad kyberprostorem? V prvních desetiletích kyberprostoru byl všeobecně přijímaný princip zásahu do kyberprostoru jako „**ruce pryč**“. Euforie z nového prostoru svobody vyvíjela velký tlak na politiky, aby se kontrole kyberprostoru ze strany státu obloukem vyhli, protože se obávali případných ekonomických dopadů a ztráty konkurenceschopnosti.[87] Tehdejším principem bylo, že toto prostředí bude spravováno pouze soukromými subjekty, nikoli státem.[88] V těchto časech byl internet tvořený hlavně „pionýry té doby“, aby reflektoval jejich hodnoty: otevřený, nikoli hierarchický, proti-autoritářský a protivládní.[89]

Jak uvádí Lewis, v letech po vzniku internetu a kyberprostoru společnost tíhla k názoru, že by měl stát do kyberprostoru zasahovat minimálně, a že tempo změn v kyberprostoru je tak veliké, že jej zkrátka **nelze zachytit** na úrovni legislativy a mezinárodních norem. Ukázalo se však, že tempo není tak zběsilé a že i státní autority mohou kyberprostor úspěšně tvarovat. Podobně panoval názor, že hranice kyberprostoru

---

[87] LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs* [online]. 2010, **16**(2), 55-65 [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/16.2_Lewis.pdf s. 56

[88] IRA MAGAZINER. *Democracy and Cyberspace: First Principles* [online]. 1998 [cit. 2016-07-28]. Dostupné z: http://web.mit.edu/m-i-t/conferences/democracy/session4.html
and Digital Media, Massachusetts Institute of Technology, Cambridge, 8 May 1998.

[89] LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs* [online]. 2010, **16**(2), 55-65 [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/16.2_Lewis.pdf s. 56

neexistují a s nimi i vymahatelnost práva v něm. Dnes státy dokázaly, že to byl z valné části omyl.[90]

S tím, jak internet zahrnoval více a více oblastí lidské činnosti, stával se pro národní bezpečnost stále více důležitějším. Soukromý sektor nebyl podle Lewise schopen kyberprostor zabezpečit a bezpečnost v něm jakožto veřejný statek proto musel **zabezpečit stát**. Éra nedotknutelnosti a nemožnosti omezit kyberprostor státem skončila a internet se stal příliš velkým na to, aby se organizoval zevnitř.[91]

Dnes se již bere ingerence státu do kyberprostoru jako více méně samozřejmá. Healey například přímo **předjímá odpovědnost státu** za bezpečnost kyberprostoru v jeho hranicích. Tím, že by stát ignoroval (obecně či pro jiné státy) nebezpečné uzly a centra nacházející se na jeho území, by přebíral část odpovědnosti za případné útoky, ohrožení a škody. Stát má podle něj povinnost dohlížet na pořádek ve svém kyberprostoru. A nabízí i způsob, jak se vypořádat s problémem přisouzení. Není podle něj nutné jít až na nejnižší technickou (Libického první vrstvu) úroveň identifikace útočníků. Naopak právě prostřednictvím odpovědnosti daného státu na něj lze působit a přimět ho k zastavení či vyšetřování útoku. Ať již nabídkami či hrozbami. V závěru však dodává, že USA jakožto zdroj největšího počtu útoků by měly nést hlavní zodpovědnost, a to právě pro svou **internetovou svobodu**, tedy nízké zasahování, které je nutně s bezpečností ve sporu.[92]

Je nepochybné, jak uvádí Deibert a Rohozinski,[93] že právě **sekuritizace kyberprostoru** přispěla k zásadní změně ve vnímání míry, jakou může stát zasahovat do

---

[90] LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs* [online]. 2010, **16**(2), 55-65 [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/16.2_Lewis.pdf s. 57

[91] Ibid. s. 58

[92] HEALEY, Jason. The Spectrum of National Responsibility for Cyberattacks. *Brown Journal of World Affairs* [online]. 2011, **18**(1) [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/181/spectrum-national-responsibility-cyberattacks s. 50-51

[93] DEIBERT, Ronald J. a Rafal ROHOZINSKI. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* [online]. 2010, **4**(1), 15-32 [cit. 2016-07-28]. Dostupné z: http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/abstract s. 14

kyberprostoru. Důvod je nasnadě, kyberprostor se stal jednou z priorit národní bezpečnosti.

Problematikou suverenity státu v kyberprostoru se zabýval také Patrick Franzese[94], podle něhož je kyberprostor součást našeho reálného světa a tedy subjekt jeho zákonitostí a řádu – tedy i subjekt, na nějž lze uplatňovat **státní suverenitu**. Například uvádí, že jakákoli data uložená na serverech společnosti Google, bez ohledu na jejich fyzickou polohu, spadají pod účinnost zákona „US Patriot Act", upravujícího mimo jiné sdílení dat důležitých pro národní bezpečnost s vládou USA, proto, že je tato firma registrována ve Spojených státech.[95]

Průnik státu do kyberprostoru je tedy evidentní, liší se jen jeho míra. Všechny **státy dnes zasahují** do kyberprostoru více, než tomu bylo před deseti lety. Jsou k tomu vedeni potřebou kontroly disentu a opozice, ochranou národní či územní suverenity či jen reagují na sílící volání po regulaci zneužívání práv duševního vlastnictví, ochrany dětí či projevů sympatie k terorismu.[96]

Organizace OpenNet Initiative ve spolupráci s univerzitou v Torontu, Harvardskou univerzitou a skupinou SecDev zdokumentovala kontrolu kyberprostoru státem v 70 zemích světa, z nichž 40 nějakým způsobem filtruje obsah internetu. Podle jejich studie bylo pod nějakou formou **státní kontroly** na 960 milionů uživatelů internetu, celých 47 %.[97]

Když Snowden odtajnil praktiky NSA a dalších agentur týkající se masového sledování obyvatel USA, ale i dalších států, prostřednictvím přímé kontroly uzlů

---

[94] FRANZESE, Patrick W. *Sovereignty in Cyberspace: Does it Exist?* [online]. 1. Air University (U.S.): School of Advanced Air and Space Studies, 2009 [cit. 2016-07-28]. Dostupné z: https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

[95] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 5

[96] Ibid. s. 7

[97] ONI TEAM. Global Internet filtering in 2012 at a glance. In: *OpenNet Initiative* [online]. 2012 [cit. 2016-07-28]. Dostupné z: https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

(infrastruktura), či spoluprací s nimi (velké společnosti jako Facebook, Google, Microsoft a další), ukázalo se, že u většiny uživatelů **nevyvolává kontrola** shora takovou nelibost, jak bychom očekávali.[98] Bauman to vysvětluje třemi důvody, které nás jako uživatele udržují na síti i přes tato rozrušení vyvolávající odhalení: 1) všedností sledování, které je tak všudypřítomné, že jej lidé už ani nevnímají, 2) strachem, ospravedlňujícím činnost bezpečnostních složek, spočívající v masovém sledování, a 3) zábavností, jakou kyberprostor přináší.[99] Vzhledem k množství hrozeb, kterým současný mezinárodněpolitický diskurz přisuzuje váhu, a kterým politici a média sekuritizací přisoudili prioritu v oblasti bezpečnosti a především vzhledem ke schopnosti bezpečnostních orgánů zvýrazňovat některé hrozby nad jiné, a tím posouvat naši potřebu bezpečnosti na výsadní pozici, dochází k tomu, že co nám dříve připadalo autoritářské, dnes vnímáme jako schůdné, či **dokonce normální**.[100]

Pokud hovoříme o vlivu státu na centra, je třeba rozlišovat přístup liberálních demokracií a ostatních států, jejichž etické a morální pohledy se mohou vzájemně značně lišit. S nimi se liší i hranice, za které hodlají při kontrole a vměšování se do center ve jménu národních zájmů zajít.

Liberální demokracie obvykle vstupují do kyberprostoru kvůli porušování práv duševního vlastnictví, zneužívání dětí, potírání nenávisti, radikalismu a islamismu. Některé státy jako Nizozemí, Francie či Velká Británie rovněž nařizují odpojení uživatelů prostřednictvím ISP, pokud sdílí nelegální obsah. **Autoritářské státy** pak zasahují rovněž kvůli potírání menšin, náboženských hnutí, politické opozice a skupin hájících lidská práva. Nicméně filtrování informací na internetu se kvůli všem možným důvodům stalo celosvětovou normou.[101]

---

[98] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 141

[99] Ibid. s. 141

[100] Ibid. s. 137

[101] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 7

V rámci vytváření strategie státu by měla být definována jeho **pozice v rámci kyberprostoru**. Stát by v ní měl odpovídat na otázky uvedené na začátku této kapitoly, více se soustředit na roli center a vymezit, zda bude řešit jejich fungování, zda se do nich bude vměšovat, či jakou roli bude hrát při jejich kontrole. Neměl by se při tom omezovat pouze na kontrolu jejich zabezpečení, ale také, jaký vztah k nim zaujme.

V druhé části práce jsou v předchozích kapitolách probrané vlastnosti center aplikovány na současnou podobu vztahů mezi státem a centry v kyberprostoru.

4. Projekce státní moci do center kyberprostoru

Pokud na základě minulé kapitoly připustíme, že stát má do jisté míry oprávnění, volbu či dokonce povinnost zasahovat do kyberprostoru, je třeba analyzovat možnosti a výzvy, které to pro něj přináší. Stevens vyjmenovává čtyři oblasti, ve kterých lze získat kontrolu nad kyberprostorem: *normy*, *kód*, *trh* a *fyzická architektura*.[102] Pro účely práce však bude vhodnější projekci státní moci takto **nerozmělňovat**. Práce se proto zaměří na projekci státní moci do center, kterou bude analyzovat prostřednictvím různých náhledů na kyberprostor.

Dosud byla v práci vymezena výjimečná role center a možné nahlížení na bezpečnost kyberprostoru s mnoha okolnostmi, které přináší. Přijmeme-li hypotézu, že na základě Barabásiho teorie sítí budou centra dále sílit a kyberprostor bude více tíhnout k hierarchické topologii, nabízí se využít jejich *vlastnosti* ve prospěch kybernetické bezpečnosti státu, či alespoň brát jejich roli při vytváření kybernetických strategií v úvahu. Je-li centrum v daném náhledu na kyberprostor pro stát významné, měl by se stát ve své strategii zabývat tím, **zda jej má pod kontrolou** a zda v sobě toto centrum nekoncentruje v důsledku růstu sítě více moci, než by odpovídalo národním zájmům.

Jak jsou centra vnímána **dosavadními strategiemi kybernetické obrany**? Důvod, že se autorovi nedařilo najít vhodné uchopení, vedl ke změně výzkumné otázky této práce. Obecně totiž strategie akcentují spíše oblasti, na které je třeba zaměřit své úsilí, jako je například spolupráce s mezinárodními organizacemi, vzdělávání a pomoc akademického sektoru, budování kapacit či spolupráce se soukromým sektorem. Mimo to se objevují kapitoly o zvyšování ostražitosti nebo snižování kybernetického zločinu. O podobných tématech mluví i strategie kybernetické obrany Evropské unie,[103] která také klade důraz na význam spolupráce se soukromým sektorem.

---

[102] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 164

[103] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *European External Action Service* [online]. 2013 [cit. 2016-05-12]. Dostupné z: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. s. 6.

Národní strategie kybernetické bezpečnosti USA z roku 2003 ve svém výčtu mezi zájmová centra řadí veřejné i soukromé instituce v zemědělství, vodohospodářství, zdravotnictví, v integrovaném záchranném systému, vládě, obranném průmyslu, informačních a telekomunikačních technologiích, energetice, dopravě, bankovnictví a finančnictví, chemickém průmyslu a nakládání s nebezpečnými materiály, poštovních a kurýrních službách.[104]

Systematičtější přístup k centrům však strategie neobsahují, a proto se práce pokouší na následujících stránkách jeden z pohledů nabídnout. V následující kapitole budou strukturovaně popsány možnosti, jaké v souvislosti s přístupem k centrům přicházejí v úvahu a vůči nimž by měl stát v kybernetické strategii **zaujmout stanovisko**.

4.1 Identifikace center

V prvé řadě se nabízí, aby se stát zabýval tím, jaká centra v jednotlivých náhledech kyberprostoru jsou pro něj relevantní a mohou nějakým způsobem ohrozit jeho národní zájmy. Měl by proto centra (ne nutně shodná s kritickou informační infrastrukturou), **identifikovat** a určit míru jejich kontrolovatelnosti. Tedy jaký má centrum význam, čím je pro stát důležité a zda toto centrum pro stát nepředstavuje hrozbu. V identifikaci mohou hrát roli například tajné služby, které by to měly jako jeden ze svých úkolů a upozorňovaly by příslušné úřady na roli některých uzlů a jejich možné ovládání či využívání cizí mocí. V každé klíčové oblasti by měla být analyzována daná centra, jejich vlastnická struktura a napojení na možné další aktéry s analýzou možného zneužití. Toto zhodnocení by mělo být provedeno i přesto, pokud by v následujícím bodě stát rozhodne, že nehodlá do kyberprostoru jakkoli zasahovat.

4.2 Míra státní ingerence do center

Již Deibert[105] vyzýval, aby se v kybernetických strategiích objevilo stanovisko státu k míře zasahování do kyberprostoru, neboť z něj následně vycházejí další opatření.

---

[104] *The National Strategy to Secure Cyberspace*. Morgan James Publishing, 2003. ISBN 9780976090144.
[105] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 15

A také pohled na kontrolu uzlů; kybernetická strategie by měla v návaznosti na ústavu a státní zřízení vyjasnit **pozici státu k centrům**, jakožto důležitým uzlům kyberprostoru, jejichž kontrola (ve smyslu ovládnutí) může být objektem národní bezpečnosti. Práce proto navrhuje, aby strategie vymezovaly, jak hodlají přistupovat k relevantním centrům, zda stát připouští nějakou formu zasahování do center, co je pro něj ještě přijatelné vměšování a co již nikoli a v jakých oblastech (např. kontrola opozice, internetové pirátství, viry vyvíjené soukromými firmami jako „kybernetické zbraně“, dětská pornografie, atd.).[106] V této souvislosti je například diskutováno, zda neomezit na svém území vývoj software, jež slouží méně demokratickým státům ke státní kontrole.[107] Dlužno podotknout, že určité základní principiální vymezení (hlavně ve vztahu k demokracii a lidským právům) se například ve strategii ČR objevuje.[108]

4.3 Formy spolupráce a kontroly nad centry

V rámci této podkapitoly jsou shromážděny **formy kontroly** (orgány či nástroje – legislativní, soudní, správní apod.), jež může stát používat v oblasti dohledu nad těmi centry, která jsou pro něj dosažitelná (tj. převážně soukromé subjekty). Postoj státu k přípustným formám kontroly by měl být uveden v kybernetické strategii.

Vztah ke kontrole soukromých subjektů napříč státy se různí. Výzvě čelí především mezinárodní firmy, obvykle ta největší centra, aby vyhověly jednak svým vnitřním morálním a etickým principům a zároveň místnímu právu v jednotlivých státech. Obzvláště složitá je situace v oblasti ochrany lidských práv, kde společnosti jako Google, Microsoft, Yahoo!, Twitter, Facebook a další čelí vzrůstajícímu tlaku, aby balancovali na

---

[106] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 7

[107] Ibid. s. 23

[108] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-04-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf s. 9

hraně mezi lukrativním trhem a s ním související nutností být v souladu s místním právem, a naopak respektováním svobody slova a svobodného přístupu k informacím.[109]

Najít **vhodný model spolupráce** mezi státním a privátním sektorem se v oblasti kybernetické bezpečnosti jeví větší výzvou, než se na první pohled může zdát. A dopad je značný, neboť ve většině zemí spravuje privátní sektor až 85 % infrastruktury související s národní a ekonomickou bezpečností. Důležitost velkých uzlů, které jsou vlastněné soukromými subjekty je i v tom, že ochrana kritické infrastruktury je ve značné části kybernetickými strategiemi[110] ukládána právě těmto centrům. Roli hraje i nadsazování případných hrozeb, jež v této oblasti posiluje trh.[111] „Strategie kybernetické bezpečnosti USA přímo vybízí k inovacím v soukromém sektoru, protože kritická infrastruktura je přirozeně provozována právě soukromými korporacemi a jejich provoz je i v jejich čistě obchodním zájmu."[112]

Uvažujeme-li o zásahu státu do soukromých center, jeví se jako nutné zvažovat, jakou mají mít soukromé subjekty odpovědnost za obsah, který jim malé uzly dodávají (což bývá také důvodem, proč se staly tak velkými centry – dík patří právě obsahu dodanému běžnými uživateli). Jak se tato centra více a více prosazují v kyberprostoru, jejich aktivity jsou pod stále větším státním dohledem a tlakem na spolupráci.[113]

---

[109] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 5

[110] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-04-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf s. 10

[111] CAVELTY, Myriam D. *Cyber-security and threat politics US efforts to secure the information age*. Oxon: Routledge, 2008 [cit. 2016-07-28]. ISBN 02-039-3741-4.

[112] SCHMIDT, Nikola. Kybernetické útoky na kritickou infrastrukturu a role standardizace v její ochraně. *Časopis 112* [online]. 2014, **13**(3) [cit. 2016-07-28]. Dostupné z: http://www.hzscr.cz/clanek/casopis-112-2014-casopis-112-rocnik-xiii-cislo-3-2014.aspx?q=Y2hudW09Nw%3D%3D

[113] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 5

Jelikož úlohu v této spolupráci často hrají tajné služby, upozorňuje Bauman na plíživou změnu v jejich vnímání transparentnosti vůči společnosti. Shrnout to lze postojem zpravodajských služeb, jež hlásá, že „bezpečnost kyberprostoru je příliš citlivé téma, než aby lidé mohli znát, co pro ně jako stát děláme a sami rozhodnout, zda je to, co děláme, správné."[114]

4.3.1 Výzva ke spolupráci

Prvním způsobem působení na centra je určitá politická výzva či tlak. Velmi známý je případ vyšetřování teroristického útoku v San Bernardinu, kdy Apple odmítl spolupracovat se státními vyšetřovateli na dešifrování iPhonu pachatele. Ocitl se pod velkým tlakem ze strany státních představitelů (a dokonce i u soudu), ale naopak našel zastání u mnoha občanů.[115] Obdobně čelil tlaku RIM, výrobce telefonů značky Blackberry, aby státům jako jsou Spojené arabské emiráty, Indie či Indonésie vyhověl a modifikoval své produkty za účelem lepší kontroly tamními orgány.[116] Jak bylo řečeno, tlak na tyto společnosti ze strany států je nutí vybrat si mezi potenciálně vynuceným odchodem z daného trhu nebo zklamáním důvěry jeho uživatelů. Ostatně RIM nakonec požadavkům vyhověl a bylo to na úkor jeho dalšího růstu.[117]

Jiný příklad výzvy můžeme vidět v požadavku vlády USA na sociální síť Twitter, o odložení plánované odstávky služby, aby se díky ní mohly koordinovat protivládní demonstrace a disidenti během protestů v Íránu.[118] Tím jej USA jako státní subjekt považovali za tak důležitého aktéra, aby intervenovaly a ovlivnily jeho vnitřní rozhodnutí

---

[114] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 137

[115] GROSSMAN, Lev. Inside Apple CEO Tim Cook's Fight With the FBI. In: *Time* [online]. 2016 [cit. 2016-07-28]. Dostupné z: http://time.com/4262480/tim-cook-apple-fbi-2/

[116] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 7

[117] Ibid.

[118] PLEMING, Sue. U.S. State Department speaks to Twitter over Iran. In: *Reuters* [online]. 2009 [cit. 2016-07-28]. Dostupné z: http://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616

ve jménu národních zájmů, navzdory přesvědčení prezidenta Obamy, že by neměly zasahovat do íránských vnitřních záležitostí.[119] Spojené státy se tak podobně jako Brazílie[120] snažili prostřednictvím kontroly nad daným uzlem prosadit národní zájmy.

Tento model udržování základního vlivu nad uzly je zřejmě nejmírnější a pro liberální demokracie by měl být v odůvodněných případech **schůdným řešením**. Neposkytuje však záruky, že dané centrum výzvě vyhoví.

4.3.2 Státní audit

Druhým způsobem vlivu státu nad centry je jejich audit ze strany státních nebo certifikačních orágnů. Zajímavý je například pohled, jakým způsobem je společnost Huawei kontrolována ve Velké Británii. Zřízeno bylo středisko pro dohled nad touto firmou, avšak financování a zaměstnance dodává sám Huawei.[121]

Stevens podkládá otázku, zda tento případ může být **jednou z možností**, jak do budoucna budovat vztah privátních a státních subjektů v oblasti kontroly kyberneticky významných center. Podíváme-li se na tento jev ve vztahu k Snowdenovým dokumentům a tím, jak vnímá situaci Bauman[122], který kritizuje přílišné propojení tajných služeb a soukromých společností, je třeba možnosti takové spolupráce detailněji diskutovat a ptát se, kdo by měl být případně tím „certifikačním orgánem" – tajné služby, bezpečnostní úřady, centra kybernetické bezpečnosti? A také je třeba vidět druhou stranu mince spočívající ve využívání takového modelu auditu méně demokratickými státy ke kontrole „západních" center. Nicméně jde asi o **nejlepší řešení** v mezích etických principů, jež

---

[119] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 160

[120] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 140

[121] STEVENS, Tim. Keeping tabs on Huawei raises awkward questions for everyone. *The Conversation* [online]. 2013 [cit. 2016-07-28]. Dostupné z: https://theconversation.com/keeping-tabs-on-huawei-raises-awkward-questions-for-everyone-21622

[122] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 140

zároveň poskytuje určitě záruky, že dané centrum bude jednat v mantinelech národních zájmů daného státu.

Růst center vede k určité centralizaci sítě. Jak bylo popsáno, stoupá moc uzlů. Způsobem, který by mohl být liberálním demokraciím více vlastní, může být tzv. **distribuovaná bezpečnosti** dle Deiberta.[123] Ten nabádá ke snížení moci center nikoli jejich náhradou, nýbrž vytvořením vícero partnerů - autorit, které by dozorovaly vždy daný okruh center v mezích zákona. Tím by se snižovala moc center ani by se moc nekoncentrovala do jedné státní autority. Tento model by vedl kyberprostor směrem k rozptýlené síti.

4.3.3 Spolupráce se státem

Nejsilnější forma ingerence státu do centra (vynecháme-li jeho plné převzetí) je přímá (či dokonce vynucená) spolupráce centra se státem. Tento model čelí silným kontroverzím nejen v souvislosti s využíváním v autoritářských státech, ale rovněž v liberálních demokraciích (jak bude uvedeno dále). Poté, co byly soukromé subjekty přibrány, aby se účastnily snahy o bezpečnější kyberprostor, **zamlžila se hranice** mezi privátním a státním a rozostřila se odpovědnost civilních a státních struktur. Nabízí se vážné otázky, jako například kam až sahá odpovědnost soukromých subjektů za kritické oblasti národní bezpečnosti.[124]

Kontroverzní spolupráce centrálních uzlů se státem vyšla najevo po úniku tajných materiálů z amerických zpravodajských služeb, vynesených Edwardem Snowdenem.[125]

---

[123] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 16

[124] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 152

[125] Např. GREENWALD, Glenn. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books, 2014. ISBN 9781627790741.

Jev byl hlouběji popsán v práci Zygmunta Baumana a jeho kolegů *After Snowden,*[126] která analyzovala dopady sledování na diskurz bezpečnosti úzce spjaté s kyberprostorem. Bauman postupně ve své práci rozebírá role velkých soukromých společnosti provozujících největší uzly v kyberprostoru a zpravodajských služeb, které je svým konáním **ovlivňují**.

Bauman klade v souvislosti se Snowdenem zajímavou otázku: Jaký je zdroj legitimity organizací masově sledujících své občany ve jménu politické potřebnosti a bezpečnosti?[127] Nejprve hovoří o tzv. **hybridizaci**, tedy stírání soukromého a veřejného sektoru, [128] jež je důsledkem blízké spolupráce center a tajných služeb.

Prolínání veřejného a soukromého sektoru není zřejmě nikde tak znatelné jako v kyberprostoru. Nalezneme v něm jak jakousi intimnost, tak naopak publicitu – veřejnost. Každý uživatel by si měl být vědom, že přes sebevětší zabezpečení své **soukromí pouští do světa**. A přesto se tak bez pozastavení stále děje a informace tak jsou k dispozici hackerům, reklamním agentům, a také státním orgánům, mnohdy jiného než vlastního státu.[129]

Hybridizace má za následek, že se tradiční oddělení národních zájmů státu od soukromého sektoru smazává. Soukromé společnosti se stávají **aktéry národní bezpečnosti**. S tímto propojením se u nich budují nástroje (například software sloužící k ukládání uživatelských dat), které je institucionálně integrují do systému národní bezpečnosti. Klíčová myšlenka Baumana spočívá v tom, že bezpečnostních agentury a jejich činnost spočívající v získávání zpravodajských informací zásahem do soukromí občanů, by měla sloužit výhradně národní bezpečnosti. Proto integrace soukromých center tento princip porušuje, čímž přispívá k erozi národního státu, jeho autority a hranic

[126] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 140
[127] Ibid. s. 124
[128] Ibid. s. 126.
[129] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf. s. 138

toho, co je přípustné vůči soukromým subjektům ve vztahu k národní bezpečnosti. Vyjmutí těchto společností z komplexního mechanismu, v rámci kterého jim bylo umožněno být součástí procesů sběru zpravodajských informací, bude v budoucnu zřejmě velmi komplikované.[130]

Hybridizace se z tohoto pohledu **nezdá vhodnou cestou** ke zvýšení kybernetické bezpečnosti. Baumanovým paradigmatem by naopak měly být uzly jednoznačně rozděleny; jsou-li pro stát dané uzly skutečně klíčové, měl by nad nimi mít kontrolu přímou. V ostatních případech by k nim měl přistupovat jako ke komerčním subjektům a nepřenášet na ně úkoly tradičně patřící národnímu státu a smyslu jeho existence.

Privatizaci pak Bauman spatřuje právě ve spolupráci těchto zpravodajských služeb se soukromými aktéry, těmi největšími uzly, které jim předávají velké množství dat o jejich uživatelích, vše pod posvěcením národní bezpečností. Nakonec Bauman rozvádí svou myšlenku do extrému, když říká: „Nebudeme příliš od pravdy, pokud naznačíme, že to, co stále nazýváme národní bezpečností, bylo **kolonizováno** novou aristokratickou vrstvou pracovníků zpravodajských agentur, která zcela samostatně operuje v nezávislé nadnárodní aréně.“[131] Rovněž Deibert volá po **větší kontrole** bezpečnostních agentur, zvlášť těch zabývajících se tzv. “big data” a signálovým zpravodajstvím (SIGINT).[132]

Takové modely jsou proto v normálních dobách „míru“ v liberálních státech velmi kontroverzní. Stát, který by k takové spolupráci přistoupil, by musel mít dostatečný důvod a poskytnout dostatečné záruky, že hranice této spolupráce nebudou ani jednou stranou překračovány a že státní orgány na ní se podílející, budou pod státní kontrolou. Opačná situace může nastat v dobách krize, kdy řízení úkolů důležitých pro občany obvykle přebírá stát. Tento model se nabízí jako **krizové řízení uzlů** a zároveň další

---

[130] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf.

[131] Ibid. s. 124

[132] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 18

možnost zlepšení kybernetických strategií. Vytváření krizových scénářů je důležitý úkol pro případ, že věci přestanou fungovat.

4.4 Postup vůči nedosažitelným centrům

V předchozí podkapitole byly zmíněny různé příklady dobrovolné či vynucené spolupráce státu a jednotlivých center. Ne na všechny, ale může mít stát vliv a měl by se proto ve své strategii zabývat i otázkou, jak přistupovat k centrům, která představují ohrožení jeho zájmů a jsou pro něj nedosažitelná.

4.4.1 Nespolupracující centra

Předpokládá se, že soukromá sféra má zájem spolupracovat se státem na zajištění kybernetické bezpečnosti, a že bude ustanovení uvedené ve strategiích (týkající se především jejich vlastní bezpečnosti) dodržovat. Co ale když má **jiné zájmy** odlišné od státu?

Příklad lze vidět v již zmíněné kauze Apple a jeho odmítnutí pomoci při dešifrování iPhonu. Pozice Apple je však v tomto sporu v jistém smyslu unikátní, neboť dokresluje výhodu částečně uzavřené a ohraničené části kyberprostoru. Díky své obchodní politice vybudovala tato americká společnost ekosystém, jehož je prakticky jediným a neotřesitelným centrem. Jak je vidět, jeho vliv je značný a je výzvou i pro Spojené státy. Protože plně využívá svého vlivu jako centrálního uzlu a vyvolává diskuzi o autonomii center v kyberprostoru, může být zajímavé na něj nahlédnout optikou teorie sítí.

Tato problematika již přesahuje ideální model bezškálové sítě, neboť v ní musíme zohlednit například sílu vazby mezi danými uzly a schopnost centra poskytnout tak unikátní typ vazby, kterou nebude možné využít k připojení k jinému uzlu. Společnost Apple díky tomu výrazně odděluje na sebe navázané uzly od ostatních částí kyberprostoru. Vytváří kolem sebe pevnou komunitu, která je unikátními vazbami napojena pouze na tento jediný velký uzel a případná změna vazby znamená pro uživatele mnohem větší úsilí než je tomu u ostatních cizích uzlů, navázaných na jiná centra. Lze to popsat i tak, že si Apple tímto krokem uměle zvyšuje svou zdatnost, neboť nové vazby u uzlů s ním již spojených mají mnohem větší preferenci připojit se opět právě k němu, než

k uzlům jiným. Na Apple ekosystém se lze dívat i jinak než optikou ekonomickou, která mu přináší pevné vazby na uživatele, ale i optikou bezpečnostní.[133] Díky uzavřenému prostředí, ověřování a instalování aplikací přes schválené nástroje snižuje počet vazeb na jiné, potenciálně nebezpečné uzly. Vytváří tak do jisté míry ostrov[134] v kyberprostoru, jehož propojenost s ostatními uzly je nižší. Takto uzavřené shluky uzlů je mnohem snazší kontrolovat, a je také mnohem jednoduší pro ně vytvářet bezpečnostní standardy. O atraktivnosti této strategie ostatně vypovídá i to, že k Applu se postupně přidávají i další velké uzly, případně si k tomu alespoň připravují půdu. Například Tim Sweeney, vývojář počítačových her, obvinil Microsoft, že si připravuje půdu, aby obdobně jako Facebook, uzavřel svůj shluk uzlů. Jeho strategie je spočívá v tom, nejprve nabídnout poměrně otevřenou a benevolentní platformu, do které se přihlásí dostatek uživatelů a vytvoří si v ní dostatek vazeb, a následně ji postupně uzavírat, aby uzly své vazby nemohly jen tak změnit.[135]

Důsledky pro strategii kybernetické bezpečnosti jsou zřejmé. Vytváření shluků, které mají dostatečně **unikátní vazby**, může být jedním ze způsobů, jak tento shluk lépe bránit, lépe kontrolovat a lépe jej ovládat. A rovněž vybudovat velmi silné centrum, které má v dané sítí postavení hegemona a může si dovolit čelit i zásahům ze strany státu. Ostatně pokud dnes chceme vytvořit skutečně bezpečnou část kyberprostoru, vytvoříme jednoduše air-gap síť. Ta je zcela odříznutá od internetu, což ji umožňuje dokonale zabezpečit a ovládnout. U velkého množství uzlů by toto řešení bylo neefektivní, ale přesto může být zkvalitňování či odlišování vazeb mezi uzly užitečnou strategií, jak zvyšovat kybernetickou bezpečnost. Odlišování vazeb mezi uzly může představovat například autentifikace uživatelů pomocí specifických nástrojů (věcí, znalostí nebo biometrických údajů).[136] Jejich používání vídáme dnes v elektronickém bankovnictví,

---

[133] LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html s. 325

[134] Příloha 4

[135] Microsoft wants to monopolise games development on PC. We must fight it. *Theguardian.com* [online]. [cit. 2016-05-12]. Dostupné z: https://www.theguardian.com/technology/2016/mar/04/microsoft-monopolise-pc-games-development-epic-games-gears-of-war

[136] HOWARD, Richard. *Cyber security essentials*. Boca Raton, FL: Auerbach Publications, 2011. ISBN 9781439851234. s. 2.

kde unikátnost vazby (připojení do systému) zabezpečené autorizací uživatele představuje účinný způsob ochrany.

4.4.2 Centra pod kontrolou cizí moci

Velké uzly, tedy centra mají moc, kterou lze zneužít ve smyslu, kdy je centrum **využíváno cizím státem** za účelem prosazení jeho národních zájmů. Podíváme-li se na Libického první vrstvu kyberprostoru, nalezneme příklad opět ve společnosti Huawei, která, jak bylo zmíněno, byla ve Velké Británii pod dohledem britské zpravodajské služby GCHQ a tedy spolupracovala se státem. V USA však byla rovnou vyřazena z možnosti ucházet se o zakázky na státní informační infrastrukturu a upřednostněny tak byly jiné společnosti = centra.[137] Česká republika má velkou část telekomunikačních sítí od Huawei, a proto by se případné zamyšlení v kybernetické strategii nad vztahem k tomuto centru nabízelo. A zkoumání by mělo být uloženo relevantním státním orgánům. Důvod je jasný: nedostat se do situace, kdy budou důležitá centra kyberprostoru zcela mimo kontrolu státu. Ze zprávy BIS vyplývá, že tuto problematiku sleduje.[138] S tímto bodem úzce souvisí i následující.

4.4.3 Centra umístěná v cizím státě

Tyto uzly spadají pod suverenitu cizího (nespolupracujícího) státu a mohou ohrožovat národní zájmy například v souvislosti s hybridní válkou, tedy souborem nasazení konvenčních sil, sabotáží a špionáže v kombinaci s masivní propagandou. Tato propaganda může probíhat prostřednictvím velkých center, která jsou **mimo kontrolu** daného státu – zpravodajské servery, sociální sítě, atp.

Jak **velkou roli** mohou mít lze ilustrovat například na sestřelení letounu MH17 nad východní částí Ukrajiny – Boeing 777 společnosti Malaysian Airlines s 298 pasažéry na palubě. Ukrajina a Západ přišel s množstvím důkazů o zapojení ruské armády do bojů

---

[137] INKSTER, Nigel. Chinese Intelligence in the Cyber Age. *Survival: Global Politics and Strategy* [online]. 2013, **55**(1), 45-66 [cit. 2016-07-28]. Dostupné z: https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-february-march-2013-3db7/55-1-05-inkster-936c s. 45–66 či Stevens, T 2013, 'Huawei-Imperial plan renews Chinese cyber-security fears', The Conversation, 05 July. https://theconversation.com/huawei-imperial-plan-renews-chinese-cyber-security-fears-15788

[138] Výroční zpráva bezpečnostní informační služby za rok 2014. In: *Bezpečnostní informační služba* [online]. 2014 [cit. 2016-07-28]. Dostupné z: https://www.bis.cz/vyrocni-zprava6c8d.html?ArticleID=1096

na Ukrajině, mimo jiné i o dodávce protiletadlových systémů, z nichž jeden byl ze sestřelu podezřelý. Ruské zpravodajské servery naopak rozšířily zprávu o svědectvích, potvrzujících přítomnost letadla ukrajinského letectva Su-25 v den tragédie. Obě strany měly svá stanoviska a začal střet propagandy v kyberprostoru.[139] Především možnost interakce, okamžité zpětné vazby a odpovědi na reakci druhé strany přinesly nový rozměr do využívání center a na ně napojených uzlů. A mezi tato centra lze počítat jak zpravodajské servery, blogy, oficiální stanoviska vlád a vyšetřovatelů a na ně navázané tiskové kanceláře, významné politické osobnosti a další vlivné osoby na sociálních sítích. Zkrátka všechny uzly, které si k dané události vytvořily vazbu, a byly dostatečně velké, aby ovlivnily mnoho dalších.

V hypotetické situaci, kdy by daný stát zcela ovládal velký uzel s velkým množstvím vazeb, mohl by **kontrolovat veřejné mínění** většiny uživatelů. Nejen, že by mohl provoz na síti sledovat, ale mohl by jej přímo měnit nebo dokonce vytvářet.

Z pohledu teorie sítí je v tomto náhledu kyberprostoru patrný vliv center nad uzly. Můžeme zde vidět rozdílné dopady činnosti center na rozhodování uzlů o tom, k jakým dalším vazbám se připojí. Čím zásadnější informaci centrum zveřejní, tím se mu pravděpodobně **zvedne zdatnost** a nejspíše přiláká i nové vazby. Z Barabásiho pravidla „bohatí bohatnou, chudí chudnou“ lze jednoduše dovodit, že s přibývající popularitou se počet nově připojovaných uzlů bude zvyšovat.

Po představení center, jaká mohou být mimo dosah státu, je možné vyjmenovat i možná protiopatření, která vyplývají z teorie sítí:

4.4.4 Vytvoření vlastních center

Jednou z možností, jak může stát čelit vzrůstající moci center je logicky **decentralizace**. Takové vnímání kybernetické bezpečnosti může být například postaveno na snižování závislosti jednotlivých států na velkých mezinárodních uzlech. Cílem je jejich duplikace, vytvoření vícero uzlů s ambicí stát se centrem - tedy decentralizace. Snahou je vytvořit alternativní uzel s dostatečnou atraktivitou, který dokáže navázat

[139] Conspiracy Files: Who shot down MH17? *BBC News* [online]. [cit. 2016-05-12]. Dostupné z: http://www.bbc.com/news/magazine-35706048

dostatek uživatelů a poskytnout jim alternativu. I když se nepodaří původní centrum zcela nahradit, lze alespoň předpokládat snížení jeho vlivu na danou část sítě.

Pokus o decentralizaci můžeme najít v části americké kybernetické strategie, která uváděla, že si jednotlivé státy USA budou samy řešit některé hrozby v kyberprostoru.[140] Jiné příklady bychom mohli najít v Rusku a Číně, pokud bychom předpokládali, že se tyto státy zasadily o vzestup tamních úspěšných sociálních sítí a vyhledávačů, nezávislých na velkých centrech z USA.[141]

Zajímavý příklad nabízí ve svém článku Bauman.[142] Týká se opatření, která začaly různé státy, nespokojené s americkou politikou masového sledování, vymýšlet a zavádět za účelem omezení úniků data jejich občanů na úložiště zpravodajských služeb cizích států. První krokem bylo vystoupení Brazílie a Německa na půdě OSN se snahou revidovat termín „data subject" používaný USA, který umožňuje do sebe svou definicí zahrnout prostřednictvím podmínek ve vztazích osob k podezřelým i osoby přímo nezúčastněné, a tím rozšiřovat okruh sledovaných uživatelů. Ze strany Brazílie a Německa jde vlastně o snahu **snížit počet kroků** a tím i vazeb, ke kterým by měly mít americké zpravodajské služby přístup. Pokud jsou tedy od sebe uživatelé dva uzly (podezřelý a jeho známý), situace je v porovnání s bezpečností ospravedlnitelná. Ale se znalostí teorie sítí je každý další krok citelným zásahem do soukromí velkého množství osob, neboť díky existenci malých světů, jak o nich hovoří Barabási, narůstá toto číslo velmi strmě.

Druhým krokem byla snaha brazilské vlády bránit se masivnímu odposlouchávání ze strany Spojených států **vývojem vlastních center** – sociálních sítí, e-mailového klienta a dalších. Ve svém důsledku tak mohou být americké uzly v Brazílii oslabeny, neboť

---

[140] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 154

[141] Příloha 2 a 3

[142] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 130.

jejich vazby převezmou uzly nové – brazilské, pokud budou mít dostatečnou zdatnost nebo pokud se brazilské vládě podaří přesvědčit své občany, že se nemají nechat sledovat cizím státem (ale pouze vlastním).

Bauman správně identifikuje hráče, který má v kyberprostoru **největší vliv** a to jsou USA. Podíváme-li se na seznam nejnavštěvovanějších serverů, jasně v něm dominují servery založené v USA, či na občany USA přímo navázané.[143] V žebříčku dvaceti nejpopulárnějších webových stránek jich najdeme ve vztahu k USA hned 14. Ostatní pouze paběrkují a tak není o vlivu USA na kyberprostor pochyb. Kyberprostor je jednoznačně koncentrovaný kolem USA a vyvážit jejich centra je pro každý stát výzva (například rozvojem národních center nebo mezinárodních spojenectví).

Brazilská politika boje s hrozbou představující masivní americké sledování má proto druhou fázi spočívající v navýšení internetové konektivity, a tedy **větším propojením** Brazílie s dalšími velkými uzly v kyberprostoru tak, aby nebylo nutné přesouvat pakety přes americké území, ale vzniklo přímé propojení. Brazílie velmi dobře pochopila roli center v síti velice dobře a přišla hned se dvěma kroky, jak snížit svou závislost na amerických uzlech.

I v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 lze najít záměr o vytvoření cloud computingových služeb, které budou určené **pro spravování státem**. Na rozdíl o výše uvedené Brazílie však půjde právě pouze o ochranu státního sektoru, nikoli občanů samotných.[144]

V podobném duchu zkouší nizozemské státní autority držet vládní data mimo dosah amerických společností, zatímco Evropská unie diskutuje o možnostech oddělení evropských informací od amerických technik dolování dat a německá vláda zkouší alespoň varovat uživatele internetu na svém území ve chvíli, kdy jejich data opouští evropský kybernetický prostor. Technologické prvky kyberprostoru, od počítačových

---

[143] Viz příloha 2: The top 500 sites on the web. *Alexa.com* [online]. [cit. 2016-05-11]. Dostupné z: http://www.alexa.com/topsites a příloha 3: Top 50 sites in the world for all categories. *Similarweb.com* [online]. [cit. 2016-05-11]. Dostupné z: https://www.similarweb.com/global

[144] Akční plán k Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-05-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf s. 16.

úložišť po podmořské optické kabely, nám přinášejí svobodu komunikace, ale také větší možnost kontroly pro státní orgány.

Lze tak pozorovat snahu oslabit uzel a zároveň jeho obdobu přesunout na své území. Takzvaná neohraničenost prostoru zde získává jasné a fyzické obrysy. Fyzický přístup k největším uzlům je totiž v případě sporu dvou stran zřejmě nezbytný. Jak Bauman sám uvádí,[145] jsme toho svědky v případě Íránu a jeho „výběrovém internetu", stejně jako do značné míry v případě velkého čínského firewallu. Rusko je určitým způsobem také částečně izolováno, neboť například druhý největší tamní uzel typu sociální sítě vk.com je v zřejmě v rukách ruského státu.[146]

Celý problém má i sociální rozměr, ve kterém uživatelé kyberprostoru, ač vědomi si své otevřenosti, dobrovolně svá data nabízí velkým uzlům. Většina dat ani neprochází přímým odposlechem technické infrastruktury (směrovačů, optických kabelů) nýbrž ochotou uživatelů vkládat svá data do cloudu, i přes vědomí možného odposlechu a neméně tak ochotnou spoluprací společností, které tento cloud spravují (například Microsoft OneDrive či Dropbox) a zpřístupňují jej (nejen) americkým tajným službám. Ze Snowdenova odhalení vyplývá, že některé služby, především NSA a britská GCHQ, spolupracovali s největšími uzly kyberprostoru (Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL, Apple a telekomunikační společnosti BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel a Interroute), které jim dobrovolně či na základě přinucení státní autoritou sbíraly data o uživatelích, a tyto pak bezpečnostní složky dále zpracovávaly, spojovaly do struktur, vytvářely rizikové profily a vizualizovaly. To znamenalo získání enormního množství dat od zákazníků těchto společností a předaného zpravodajským službám bez vědomí uživatelů.[147]

---

[145] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 130.

[146] Russian social network founder says he has been fired. *BBC.com* [online]. 2014 [cit. 2016-05-13]. Dostupné z: http://www.bbc.com/news/technology-27113292

[147] BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-05-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf s. 123

4.4.5 Snižování atraktivity

Druhý způsobem jak ovlivnit centra v kyberprostoru, která jsou pro stát přímo nedostupná, je snižování jejich atraktivity. Tedy například informováním běžných uzlů o kontroverzích daného centra či uvádění jím vypouštěných **informací na pravou míru**. Vrátíme-li se k příkladu s propagandou na Ukrajině, spočíval by tento postup v upozorňování na cílené desinformace vysílané propagandistickými centry. Upozornění na problém a znevěrohodnění daného centra může vést k odlivu jeho vazeb (uživatelů) a tedy snížení jeho role a důležitosti.

Při polemice o vytváření vlastních center je třeba vzít v úvahu i kyberprostor, který mnoho negativních jevů jakožto sociální konstrukt **sám vyřeší**. Dokázal by tak zřejmě například rychle nahradit ztracené centrální uzly, stejně jako se přeorientuje na jiná centra, pokud je vyhodnotí atraktivnějšími. Tyto mechanismy jsou součástí samoorganizace bezškálových sítí.

Tuto schopnost je možné rovněž státem využít, pokud by stát atraktivitu cílového centra **dokázal snížit**. Ač se může zdát existence center v kyberprostoru analogická s mnoha jinými odvětvími, způsob, jakým rostou, je značně odlišuje. Jsou živeny vazbami jednotlivých uzlů, díky kterým mají takový vliv. Mimo jiné to znamená, že jim může být tato role odejmuta právě jednotlivými uzly, které se díky snížené atraktivitě daného centra přeorientují na jiné. Pokud se někomu (státu) podaří přesvědčit i občany, že dané centrum jde proti jejich zájmům, může tomuto centru způsobit značný odliv vazeb a tím snížit jeho vliv. Trh nabízí více center než jedno (už proto, že jde o decentralizovanou síť), a proto si v případě problémů síť rychle najde alternativu a problém vyřeší.

4.4.6 Další způsoby

Pro pořádek je vhodné uvést i další (z pohledu teorie sítí již méně zajímavé) způsoby, jako je 1) působení na daný stát v rámci **mezinárodních vztahů** a tedy možnost dosáhnout cíle tradičními prostředky diplomacie, 2) „zoufalá“ možností **blokování** daného uzlu, 3) **kombinace** dříve uvedených kroků, či 4) *ultima ratio* nouzové přeorientování se na centra nižší Libického vrstvy a např. **vypnutí** klíčových center první vrstvy kyberprostoru, jako tomu bylo např. v Egyptě či Libyi během tzv. arabského

jara.[148] Tato opatření ale nejsou zcela mimo realitu ani u liberálních států (např. vypnutí buňkových telefonních stanic při protestech v San Franciscu v roce 2011).[149]

Všechna výše uvedená opatření pro získání kontroly nad uzly jsou vlastní spíš méně demokratickým státům, neboť ze své podstaty působí **přímo proti** „znepřátelenému centru“. To musí zdiskreditovat, nahradit či k němu zablokovat přístup. Využívání takových metod liberálně demokratickými státy bude zřejmě společensky obhajitelné **pouze v případě sebeobrany**.

4.5 Mezinárodně sdílený pohled

Závěrečným doporučením pro možnosti zlepšení kybernetických strategií je, po vyjasnění pozice státu ke všem předchozím pohledům, jejich konzultace s **mezinárodními partnery** v rámci existujících fór. Cílem by mělo být vytvořit koalici obdobně smýšlejících států, která by výše uvedené myšlenky sdílela ve snaze je šířit v mezinárodním společenství. Stevens v této oblasti shledává nedostatky v národních strategiích či v nedostatečné mezinárodní koordinaci a shodě na nějakých principech.[150]

Stát může projektovat svou moc i pomocí tzv. „**soft power**“, kam Joseph Nye zařadil právě i ovlivnění okolních států prostřednictvím kyberprostoru. Jeho pojetí však zahrnovalo jak využití kyberprostoru k ovlivňování okolních států, tak k poškození nepřátelských systémů za účelem posílení vlastního postavení v reálném světě.[151]

Snaha zaujmout postoje ke kontrole uzlů v kyberprostoru se projevuje v rámci mezinárodní organizace s názvem **Shanghai Cooperation Organization**, která sdružuje

---

[148] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 9

[149] CABANATUAN, Michael. BART admits halting cell service to stop protests: Move to disrupt protesters' plans blasted as violation of free speech. *SF GATE* [online]. 2011 [cit. 2016-07-28]. Dostupné z: http://www.sfgate.com/news/article/BART-admits-halting-cell-service-to-stop-protests-2335114.php

[150] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 152

[151] NYE, Joseph S. *The future of power*. New York: Public Affairs, c2011. ISBN 978-1-61039-069-9.

země jako Čínu, Kazachstán, Kyrgyzstán, Rusko, Tádžikistán a další, jež mají mimo jiné podobný pohled na ideální míru vlivu státu v kyberprostoru. V roce 2008 vydala tato organizace prohlášení, ve kterém vyjádřila obavy o využívání dominantního postavení některých států v kyberprostoru k šíření škodlivých informací do duchovní, morální a kulturní sféry jiných států.[152] Během následujících jednání vznikla iniciativa ke sjednocení pohledů na roli státu v kyberprostoru a sdílení tohoto pohledu mezi ostatní stejně „naladěné" státy. Je třeba říci, že onen pohled je od hodnot liberálních demokracií logicky odlišný.[153]

Již tedy existuje mezinárodní společenství států, které se snaží prosadit určitý pohled na posuzování role státu v kyberprostoru, mimo jiné i při nakládání s centry tak, aby byla pod kontrolou. To je v souladu s Deibertovým tvrzením, že definování tohoto pohledu liberálními státy je nezbytné a tuto část jakési **kybernetické zahraniční politiky** by měly strategie obsahovat.[154]

Dokument „*International Strategy for Cyberspace*" uvádí, že ke kyberprostoru nelze přistupovat v oblasti mezinárodních vztahů čistě analogicky a zmiňuje se o potřebě přizpůsobit současné mezinárodní normy specifickým vlastnostem kyberprostoru berouc v úvahu základy mezinárodního práva.[155] Výše uvedený návrh může být proto jedním z příspěvků do budování těchto **kybernetických mezinárodních vztahů**.

Stevens je však k rozsáhlé mezinárodní spolupráci v této oblasti skeptický, neboť i přes budování společné kultury kybernetické bezpečnosti, státy dosud vždy budovali i

---

[152] Agreement between the members of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security. In: *Shanghai Cooperation Organization* [online]. 2009 [cit. 2016-07-28]. Dostupné z: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

[153] DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092. Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf s. 10

[154] Ibid. s. 20

[155] THE WHITE HOUSE. 2011. International Strategy for Cyberspace. Retrieved from: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspa ce.pdf.

vojenské schopnosti v kyberprostoru, například když neměly mnoho důvěry ve schopnost globálních úmluv upravujících kyberprostor odstrašit potenciálního protivníka.[156]

[156] STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764 s. 166

Závěr

Kyberprostor čelí v posledních dvou dekádách silné sekuritizaci, kdy je považován mnoha státy za jednu z **priorit národní bezpečnosti**. Vzniká proto mnoho prací snažících se popsat jeho jednotlivé aspekty. Ani tato práce nemá ambice obsáhnout problém ve své celkové komplexitě, a zaměřuje se proto jen na úzkou výseč týkající se bezpečnostní role center v kyberprostoru.

V průběhu celé práce narážíme na to, že kybernetická bezpečnost je ve velké míře spojená s uzly. Strategie kybernetické bezpečnosti na tyto uzly kladou požadavky, ale také jim předávají pravomoci, či vytvářejí příležitost, aby byly tyto uzly posíleny. Již méně se však zabývají otázkou role těchto center v jejich bezpečnosti a v tom, zda nepředstavují nějakou hrozbu. Cíle práce bylo toto napravit a poskytnout koncept, který by strukturovaně možné role center a přístupy států k nim konceptualizoval.

Práce se zaměřuje na dynamiku centrálních uzlů v kyberprostoru jako klíčových struktur v této sociální doméně. Tento přístup je přínosný zejména ke zhodnocení stále stoupajícího vlivu nových nestátních aktérů představujících tyto uzly.

V práci byla shrnuta základní role uzlů v jednotlivých **náhledech** kyberprostoru a jejich možné vzájemné vztahy se státem, ale byly zodpovězeny i další otázky rozvíjející rozměr kyberprostoru jako sociálního konstruktu: Jaké dopady má činnost uzlu na bezpečnost kyberprostoru, jakou roli v ní dané centrum hraje a jaké dopady mohou mít kroky, jež učiní. A není se nutné dívat příliš do budoucnosti. Mnohdy postačí kritická analýza událostí a procesů, které se uskutečnily před nedávnem nebo které dokonce probíhají přímo teď.

Zdroje v jednotlivých kapitolách této práce zahrnovaly nejčastěji citované autory a jejich pohledy na danou problematiku. Základním východiskem práce bylo sledovat velká centra v kyberprostoru optikou Barabásiho teorie sítí a přinést odlišný pohled na známou problematiku. Teorie sloužila jako prostředek nahlížení na problémy v literatuře diskutované ve snaze tímto náhledem přinést konceptualizovat strukturovaný návod na chování státu vůči centrům a přinést závěry, jež nejsou přímo očividné.

Cestou nabízenou v této práci je vnímat kyberprostor ve svém celku a uvědomit si klíčovou roli center pro jeho fungování. Ve všech případech byla optika, kterou před 14 lety popsal Barabási, užitečná k náhledu na problém v jiném světle. Někde přinesla zajímavá zjištění, někde jen umožnila pochopit problém z jiné strany. Aplikace teorie sice otevřela nový pohled, ale na v literatuře již probrané problémy. Prokázala však svou funkčnost, vezmeme-li v úvahu, že byla využita ve své základní podobě s ideálním modelem bezškálové sítě. Zřejmě právě proto však neposkytla hlubší výstup.

Ač se práce snažila poskytnout díky aplikaci teorie sítí nějaké zcela nové možnosti zlepšení kybernetické obrany, nedá se o novém objevu hovořit. Většina předkládaných řešení byla v odborné literatuře do jisté míry již v minulosti probrána a práce nabídla jejich uspořádání pomocí teorie do nového pohledu, který může být hoden dalšího zkoumání. Největší přínos práce by tak mělo být právě toto poskytnutí strukturovaného pohledu na roli center a možnosti jejich kontroly ze strany národních států.

Práci by bylo možné ještě rozvinout v několika směrech. Jednak v širší konceptualizaci kybernetických strategií a toho, co pro národní státy představují a přináší. Zřejmě by k tématu pasovala i analýza a definování východisek alespoň jedné z nich. V neposlední řadě byl notně zobecněn stát na teoretický konstrukt, který má však v praxi mnoho odlišností a především by bylo zajímavé představenou strukturu na vybraný stát aplikovat a otestovat její funkčnost.

Hlavní otázku, **jaké jsou možnosti zlepšení strategií kybernetické bezpečnosti**, práce operacionalizuje aplikací významu center v kyberprostoru a hodnocením vztahu státu k nim. Výsledkem je soubor doporučení, která by měla stát navést na uvažování o centrech jiným způsobem než jen o jejich zabezpečení a vybídnout jej strategicky se vůči centrům vymezit a definovat prostředky kontroly, jež jsou pro něj přijatelné a jež by si představoval, že by měly být etalonem i pro ostatní mezinárodní aktéry.

Strategie kybernetické bezpečnosti jsou snahou státu o udržení základní kontroly nad kyberprostorem a o zajištění jeho bezpečnosti. Mezi konkrétní závěry práce patří tato doporučení na jejich zlepšení:

1) Ve vztahu k rolím center v tomto sociálním konstruktu by měl stát identifikovat centra, jež jsou relevantní pro jeho národní zájmy,

2) definovat vlastní postoj k míře zasahování národního státu do kyberprostoru,

3) vymezit, jaké formy vměšování do jednotlivých center jsou pro stát přijatelné. Pro liberální demokracie práce navrhla následující hodnocení:

    a. *výzvu ke spolupráci* s centrem označila jako **schůdné řešení**, avšak neposkytující záruky,

    b. *státní audit* nebo jeho verzi *distribuovanou bezpečnost* jako **nejlepší řešení**,

    c. přímou *spolupráci centra se státem* - pouze jako **nástroj krizové řízení** a

4) vymezit postup vůči *nedosažitelným centrům* - využívání zmíněných metod **pouze v případě sebeobrany.**

Dále práce navrhuje, aby strategie upravovala otázku určení odpovědnosti za **monitorování** nebezpečí center vůči národním zájmům. Neopominout by měla otázku garance **kontroly státních orgánů**, jež budou mít na tato centra vliv (například zpravodajských služeb) a brala v úvahu rovněž možnost **zániku některých center**. Po zhodnocení všech těchto otázek a utvoření celkového obrazu o přístupu státu k významným centrům v kyberprostoru by měl stát svůj pohled diskutovat s ostatními partnery na mezinárodní scéně a ve shodě jej prosazovat u států, kteří zatím takové zhodnocení neprovedli, případně neodpovídá představě liberálně demokratického státu. Doporučení lze shrnout do výzvy, že **možností zlepšení strategie kybernetické bezpečnosti je komplexní přístup k roli center a zaujetí stanoviska vůči nim.**

Těmito doporučeními a zároveň poměrně širokou konceptualizací tří základních předpokladů práce – Barabásiho teorie sítí, kyberprostoru a role státu v něm zároveň odpovídá na otázky zmíněné v samotném úvodu práce: Jaká je úloha center v kyberprostoru? Jak je možné jejich zkoumáním vylepšit kybernetickou bezpečnost? Jak by měl stát k centrům přistupovat?

Summary

The thesis performed several probes to phenomena connected with cyberspace and its security. Developing the best approaches to tackle cyberspace strategy did not bring a unique solution. However, it shows path worth to take. One of these paths offered by this thesis is to understand the cyberspace in its complexity bearing in mind the key role of central nodes for its functionality.

Throughout the thesis we discovered the nodes-interlinked cybersecurity. These central nodes are also mentioned in relevant cybersecurity strategies and they are asked to be more involved in the national security. The more important role in security they play, the more power they acquire, the bigger power they represent.

How does this scope answer the question how defend the cyberspace? The thesis does not bring any breakthrough revelation, but offers well-structured package of questions, which a state should answer in its cyber strategy. Firstly, a state should identify any central nodes, which are relevant to its national interests. Secondly, it should take a position what is appropriate level of control of centres in cyberspace. Thirdly, it should evaluate its boundaries in order to cooperate or to force nodes to cooperation. Following that a state should develop an attitude how to deal with big nodes, which are not accessible by its direct legislative, judicial or physical power. Last but not least, concluding above outcomes, a state should develop a comprehensive approach to central nodes in cyberspace, share it with other like-minded states, discuss it and make an international standard in order to inspire other states across the world to adopt these standards.

The application of Barabási's linked theory did not bring any new ways how to improve cyberdefence, which would be completely undiscovered by scholars. However, it showed several cyberspace outlooks in a new light, explained and confirmed assumed hypothesis. In some cases, it brought interesting findings, in other cases it enabled "only" an out of the box understanding.

The main focus of the thesis is at the dynamics of the central nodes in cyberspace representing key structures in this social domain. This beneficiary attitude fits the

assessments of rising non-state actors (central nodes). The thesis summarises their roles in different paradigms of cyberspace and relationships between them and a national state.

Použitá literatura

Agreement between the members of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security. In: *Shanghai Cooperation Organization* [online]. 2009 [cit. 2016-07-28]. Dostupné z: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

ARQUILLA, John. a David F. RONFELDT. *The advent of netwar* [online]. Santa Monica, CA: RAND, 1996 [cit. 2016-07-28]. ISBN 08-330-2414-0. Dostupné z: http://www.rand.org/pubs/monograph_reports/MR789.html

ATWAN, Abdel Bari. *The Secret History of al Qaeda*. London: Saqi, 2012. ISBN 9780863568435.

BALABÁN, Miloš, Antonín RAŠEK a Martin POTŮČEK. Rodící se nová ohrožení v neklidném světě. *Vojenské rozhledy* [online]. 2011, **20**(4), 3-21 [cit. 2016-04-10]. ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/rodici-se-nova-ohrozeni-v-neklidnem-svete

BARABÁSI, Albert-László. The network takeover. *Nature physics* [online]. 2012, (8), 14-16 [cit. 2016-04-10]. Dostupné z: http://www.mamartino.com/img/Barabasi_2012_The_network_takeover.pdf

BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3.

BAUMAN, Zygmunt. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* [online]. 2014, **8**(2), 121-144 [cit. 2016-04-10]. Dostupné z: http://www.cips-cepi.ca/wp-content/uploads/2014/09/Didier-Bigo_document-Oct6.pdf

BUREŠ, Oldřich (ed.). *Bezpečnost v době neklidu: sborník vybraných příspěvků ze studentské konference pořádané v Brně 19. dubna 2013 Centrem bezpečnostních studií Metropolitní univerzity Praha, Centrem pro bezpečnostní a strategická studia*

a Oddělením pro Bezpečnostní a strategická studia Fakulty sociálních studií Masarykovy univerzity v Brně [online]. Praha: Metropolitan University Prague Press, 2013 [cit. 2016-07-28]. ISBN 978-80-86855-92-9.

CABANATUAN, Michael. BART admits halting cell service to stop protests: Move to disrupt protesters' plans blasted as violation of free speech. *SF GATE* [online]. 2011 [cit. 2016-07-28]. Dostupné z: http://www.sfgate.com/news/article/BART-admits-halting-cell-service-to-stop-protests-2335114.php

CAVELTY, Myriam D. *Cyber-security and threat politics US efforts to secure the information age* [online]. Oxon: Routledge, 2008 [cit. 2016-07-28]. ISBN 02-039-3741-4. Dostupné z: http://samples.sainsburysebooks.co.uk/9781134086702_sample_525050.pdf

CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. In: *4th International Conference on Cyber Confl ict*. Talin: NATO CCD COE Publications, 2012, s. 141-153.

Conspiracy Files: Who shot down MH17? *BBC News* [online]. [cit. 2016-04-12]. Dostupné z: http://www.bbc.com/news/magazine-35706048

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *European External Action Service* [online]. 2013 [cit. 2016-04-12]. Dostupné z: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

CZOSSECK, Christian, Rain OTTIS a Anna-Maria TALIHARM. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. *Cooperative Cyber Defense Center of Excellence Website* [online]. 2011 [cit. 2016-04-13]. Dostupné z: https://www.researchgate.net/publication/220143696_Estonia_after_the_2007_Cyber_Attacks_Legal_Strategic_and_Organisational_Changes_in_Cyber_Security

DEIBERT, Ron. *Distributed security as cyber strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* [online]. 1. Calgary: Canadian Defence & Foreign Affairs Institute, 2012 [cit. 2016-07-28]. ISBN 978-097-3787-092.

Dostupné z: https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf

DEIBERT, Ronald J. a Rafal ROHOZINSKI. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* [online]. 2010, **4**(1), 15-32 [cit. 2016-07-28]. Dostupné z: http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/abstract

DENNING, Dorothy Elizabeth Robling. *Information warfare and security*. Reading, Ma.: Addison-Wesley, c1999. ISBN 02-014-3303-6.

Department of Defense Strategy for Operating in Cyberspace. *Computer Security Resource Center (CSRC)* [online]. [cit. 2016-04-13]. Dostupné z: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

DRULÁK, Petr. *Jak zkoumat politiku: kvalitativní metodologie v politologii a mezinárodních vztazích*. Praha: Portál, 2008. ISBN 978-80-7367-385-7.

FRANZESE, Patrick W. *Sovereignty in Cyberspace: Does it Exist?* [online]. 1. Air University (U.S.): School of Advanced Air and Space Studies, 2009 [cit. 2016-07-28]. Dostupné z: https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

GREENWALD, Glenn. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books, 2014. ISBN 9781627790741.

GROSSMAN, Lev. Inside Apple CEO Tim Cook's Fight With the FBI. In: *Time* [online]. 2016 [cit. 2016-07-28]. Dostupné z: http://time.com/4262480/tim-cook-apple-fbi-2/

HEALEY, Jason. The Spectrum of National Responsibility for Cyberattacks. *Brown Journal of World Affairs* [online]. 2011, **18**(1) [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/181/spectrum-national-responsibility-cyberattacks

HOUSER, Pavel. Mocninné versus normální zákony – a co z toho vyplývá. In: *Scienceworld* [online]. [cit. 2016-04-13]. Dostupné z: http://www.scienceworld.cz/neziva-priroda/mocninne-versus-normalni-zakony-a-co-z-toho-vyplyva-1716/

HOWARD, Richard. *Cyber security essentials*. Boca Raton, FL: Auerbach Publications, 2011. ISBN 9781439851234.

HUNTER, Eva a Piret PERNIK. The Challenges of Hybrid Warfare. *International Centre for Defense and Security* [online]. Estonia, 2015 [cit. 2016-07-28]. Dostupné z: http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf

CHEN, Pin-Yu, Shin-Ming CHENG a Kwang-Cheng CHEN. *Smart attacks in smart grid communication networks*. IEEE Communications Magazine [online]. 2012, 50(8), 24-29 [cit. 2016-04-01]. DOI: 10.1109/MCOM.2012.6257523. Dostupné z: http://santos.ee.ntu.edu.tw/papers/2012/Smart%20Attacks%20in%20Smart%20Grid%20Communication%20Networks.pdf

INKSTER, Nigel. Chinese Intelligence in the Cyber Age. *Survival: Global Politics and Strategy* [online]. 2013, **55**(1), 45-66 [cit. 2016-07-28]. Dostupné z: https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-february-march-2013-3db7/55-1-05-inkster-936c

IRA MAGAZINER. *Democracy and Cyberspace: First Principles* [online]. 1998 [cit. 2016-07-28]. Dostupné z: http://web.mit.edu/m-i-t/conferences/democracy/session4.html

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. In: *Cyberpower and National Security*. Washington D.C.: National Defense University Press, 2009, s. 24-42.

LATOUR, Bruno. *Aramis, or, The love of technology*. Cambridge, Mass.: Harvard University Press, 1996. ISBN 0674043235.

LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs* [online]. 2010, **16**(2), 55-65 [cit. 2016-07-28]. Dostupné z: https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/16.2_Lewis.pdf

LIBICKI, Martin C. *Conquest in cyberspace: national security and information warfare*. New York: Cambridge University Press, 2007. ISBN 978-0-521-69214-4.

LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy for the Information Society* [online]. 2012, **8**(2), 325-340 [cit. 2016-07-28]. Dostupné z: http://www.rand.org/pubs/external_publications/EP51077.html

LUKE, Timothy W. Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace. *Spaces of Culture: City, Nation, World* [online]. 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 1999, s. 27 [cit. 2016-04-11]. DOI: 10.4135/9781446218723.n2. ISBN 9780761961222. Dostupné z: http://sk.sagepub.com/books/spaces-of-culture/n2.xml

Microsoft wants to monopolise games development on PC. We must fight it. *Theguardian.com* [online]. [cit. 2016-04-12]. Dostupné z: https://www.theguardian.com/technology/2016/mar/04/microsoft-monopolise-pc-games-development-epic-games-gears-of-war

MILGRAM, Stanley. The Small World Problem. *Psychology Today*. **1967**(2), 60-67.

MUELLER, Milton L. *Networks and States: The Global Politics of Internet Governance*. 1. Cambridge: The MIT Press, 2010 [cit. 2016-07-28]. ISBN 9780262290135.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *NATO CCD COE* [online]. [cit. 2016-04-12]. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

NYE, Joseph S. *The future of power*. New York: Public Affairs, c2011. ISBN 978-1-61039-069-9.

ONI TEAM. Global Internet filtering in 2012 at a glance. In: *OpenNet Initiative* [online]. 2012 [cit. 2016-07-28]. Dostupné z: https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

PLEMING, Sue. U.S. State Department speaks to Twitter over Iran. In: *Reuters* [online]. 2009 [cit. 2016-07-28]. Dostupné z: http://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616

RAŠEK, Antonín. Kybernetická válka pokračuje. *Vojenské rozhledy* [online]. 2013, **21**(4), 73-89 [cit. 2016-04-10]. Dostupné z: http://www.vojenskerozhledy.cz/selektivni-vyhledavani/kategorie-clanku/teorie-a-doktriny/kyberneticka-valka-pokracuje

RID, Thomas. *Cyber war will not take place*. New York: Oxford University Press, 2013. ISBN 9780199330638.

Russian social network founder says he has been fired. *BBC.com* [online]. 2014 [cit. 2016-04-13]. Dostupné z: http://www.bbc.com/news/technology-27113292

SCAPARROTTI, Curtis. *Joint Publication 3-13 Information Operations* [online]. In: Joint Publication. 2012 [cit. 2016-04-12]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

SHIFFMAN, Gary a Ravi GUPTA. Crowdsourcing cyber security: a property rights view of exclusion and theft on the information commons. *International Journal of the Commons* [online]. 2013, **7**(1), 92-112 [cit. 2016-04-10]. Dostupné z: https://www.thecommonsjournal.org/articles/10.18352/ijc.343/

SCHMIDT, Nikola. A Sociological Approach to Cyberspace Conceptualization and Implications for International Security. In: DRMOLA, Jakub (ed.). *Perspectives on Cybersecurity*. Brno: Masaryk university, 2015, s. 70-77. ISBN 978-80-210-7870-3.

SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie (Defence and Strategy)* [online]. 2014-7-15, **14**(1), 29-38 [cit. 2016-04-13]. DOI: 10.3849/1802-7199.14.2014.01.029-038. ISSN 12146463. Dostupné z: http://www.defenceandstrategy.eu/cs/aktualni-cislo-1-2014/clanky/critical-comments-on-current-research-agenda-in-cyber-security.html#.U7ZXZ1OAI_0

SCHMIDT, Nikola. Kybernetické útoky na kritickou infrastrukturu a role standardizace v její ochraně. *Časopis 112* [online]. 2014, **13**(3) [cit. 2016-07-28]. Dostupné z: http://www.hzscr.cz/clanek/casopis-112-2014-casopis-112-rocnik-xiii-cislo-3-2014.aspx?q=Y2hudW09Nw%3D%3D

SCHMIDT, Nikola. Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War. *Obrana a strategie* [online]. 2014, **14**(2), 73-86 [cit. 2016-07-28]. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/neither-conventional-war-nor-a-cyber-war-but-a-long-lasting-and-silent-hybrid-war.html#.V5VctLiLSUk

STEVENS, Tim. A Cyberwar of Ideas?: Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2016-07-28]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2100764

STEVENS, Tim. Keeping tabs on Huawei raises awkward questions for everyone. *The Conversation* [online]. 2013 [cit. 2016-07-28]. Dostupné z: https://theconversation.com/keeping-tabs-on-huawei-raises-awkward-questions-for-everyone-21622

The National Strategy to Secure Cyberspace. Morgan James Publishing, 2003. ISBN 9780976090144.

The top 500 sites on the web. *Alexa.com* [online]. [cit. 2016-04-11]. Dostupné z: http://www.alexa.com/topsites

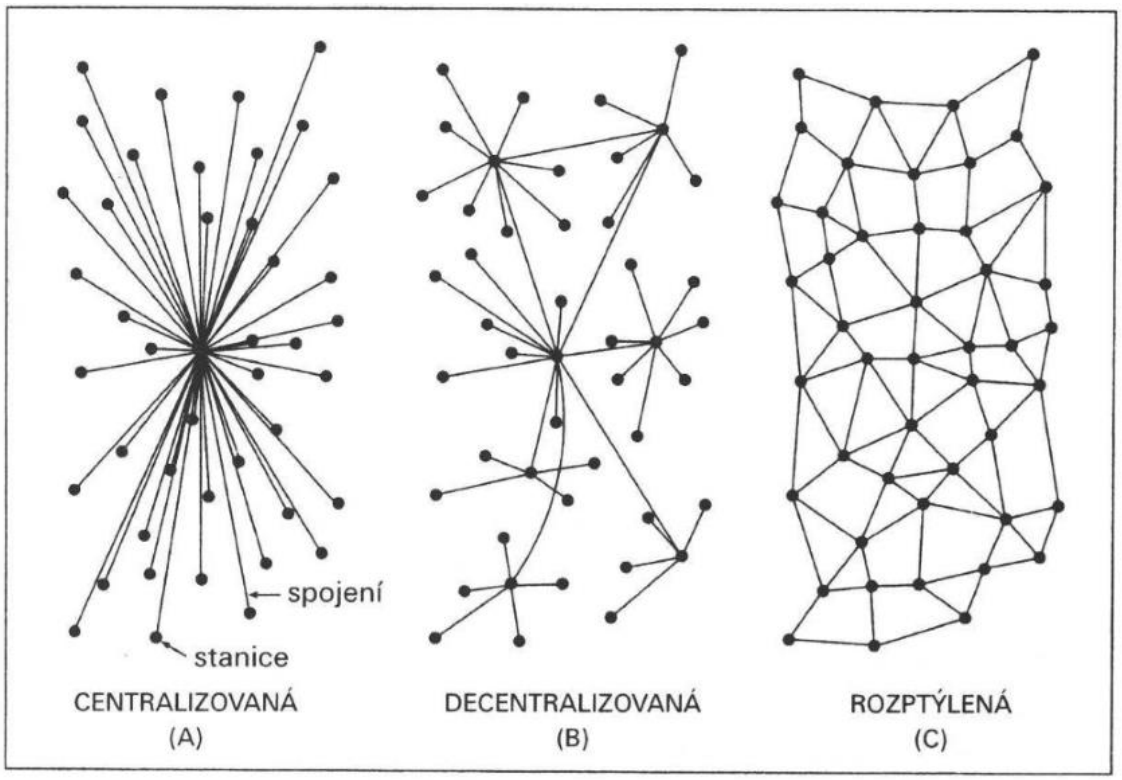
Top 50 sites in the world for all categories. *Similarweb.com* [online]. [cit. 2016-04-11]. Dostupné z: https://www.similarweb.com/global

Výroční zpráva bezpečnostní informační služby za rok 2014. In: *Bezpečnostní informační služba* [online]. 2014 [cit. 2016-07-28]. Dostupné z: https://www.bis.cz/vyrocni-zprava6c8d.html?ArticleID=1096

Seznam příloh

Přílohy

Příloha č. 1: Schéma typů sítí dle A. L. Barabásiho



Zdroj: BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3.

Příloha č. 2: Nejpopulárnější webové stránky dle SimilarWeb.com (tabulka aktuální k 4. 4. 2016)

#	Webová stránka	URL adresa	Funkce	Původ
1	Facebook	facebook.com	Social network	U.S.
2	Google	google.com	Internet services and products	U.S.
3	YouTube	youtube.com	Video sharing	U.S.
4	VK	vk.com	Social network	Russia
5	Yahoo!	yahoo.com	Portal and media	U.S.
6	Windows Live	live.com	Email, web services and software suite	U.S.
7	Odnoklassniki	ok.ru	Social Networking	Russia
8	Instagram	instagram.com	Photo sharing and social media	U.S.
9	Wikipedia	wikipedia.org	Encyclopedia	U.S.
10	Yandex	yandex.ru	Search engine	Russia
11	Twitter	twitter.com	Social network	U.S.
12	Google Brazil	google.com.br	Search engine	Brazil
13	Mail.ru	mail.ru	Web Portal	Russia
14	Amazon	amazon.com	E-commerce and cloud computing	U.S.
15	Google UK	google.co.uk	Search engine	UK
16	Baidu	baidu.com	Search engine	China
17	Google India	google.co.in	Search engine	India
18	Google France	google.fr	Search engine	France
19	Google Japan	google.co.jp	Search engine	Japan
20	Google Germany	google.de	Search engine	Germany
Celkem původ USA				**9 (+5)**

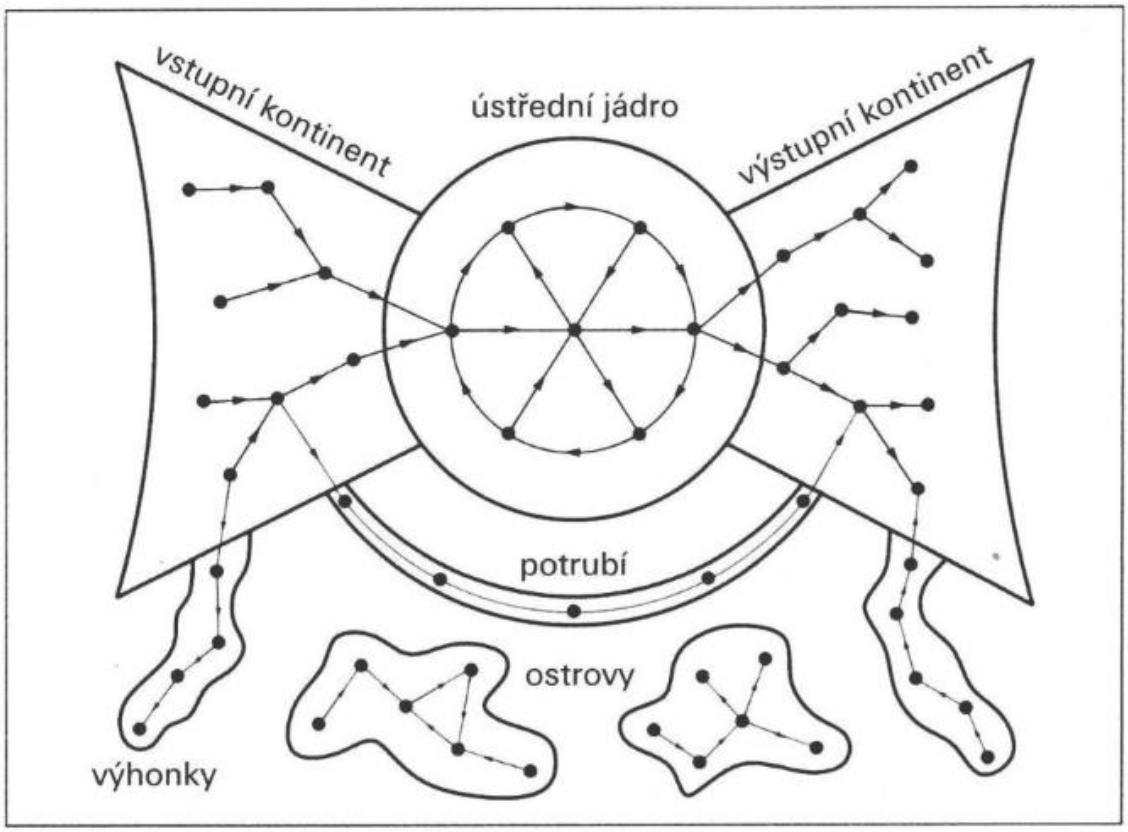
Zdroj: Top 50 sites in the world for all categories. *Similarweb.com* [online]. [cit. 2016-04-11]. Dostupné z: https://www.similarweb.com/global

Příloha č. 3: Nejpopulárnější webové stránky dle Alexa.com (tabulka aktuální k 23. 3. 2016)

#	Webová stránka	URL adresa	Funkce	Původ
1	Google	google.com	Internet services and products	U.S.
2	YouTube	youtube.com	Video sharing	U.S.
3	Facebook	facebook.com	Social network	U.S.
4	Baidu	baidu.com	Search engine	China
5	Yahoo!	yahoo.com	Portal and media	U.S.
6	Amazon	amazon.com	E-commerce and cloud computing	U.S.
7	Wikipedia	wikipedia.org	Encyclopedia	U.S.
8	Tencent QQ	qq.com	Portal	China
9	Google India	google.co.in	Search engine	India
10	Twitter	twitter.com	Social network	U.S.
11	Windows Live	live.com	Email, web services and software suite	U.S.
12	Taobao	taobao.com	Online shopping	China
13	MSN	msn.com	Portal	U.S.
14	Sina Corp	sina.com.cn	Portal and instant messaging	China
15	Yahoo! Japan	yahoo.co.jp	Portal	Japan
16	Google Japan	google.co.jp	Search engine	Japan
17	LinkedIn	linkedin.com	Professional Social network	U.S.
18	Sina Weibo	weibo.com	Social network	China
19	Bing	bing.com	Search engine	U.S.
20	Yandex	yandex.ru	Search engine	Russia
Celkem původ USA				**11(+3)**

Zdroj: The top 500 sites on the web. *Alexa.com* [online]. [cit. 2016-04-11]. Dostupné z: http://www.alexa.com/topsites

Příloha č. 4: Schéma ostrovů www dle A. L. Barabásiho



Zdroj: BARABÁSI, Albert-László. *V pavučině sítí*. V Praze: Paseka, 2005. Fénix (Paseka). ISBN 80-7185-751-3.