UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií

Katedra bezpečnostních studií

Bakalářská práce

2018 **Miroslav Crha**

UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií

Katedra bezpečnostních studií

Relevance norem v kyberprostoru

Bakalářská práce

Autor práce: Miroslav Crha

Studijní program: Politologie a mezinárodní vztahy

Vedoucí práce: PhDr. Vít Střítecký, M.Phil., Ph.D

Rok obhajoby: 2018

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 11. 5. 2018 Miroslav Crha

Bibliografický záznam

Crha, Miroslav. *Relevance norem v kyberprostoru.* Praha, 2018. 48 s. Bakalářská práce (Bc). Univerzita Karlova, Fakulta sociálních věd, Institut politologických studií. Katedra bezpečnostních studií. Vedoucí diplomové práce PhDr. Vít Střítecký, M.Phil., Ph.D.

Rozsah práce: 81 418 znaků vč. mezer

Anotace

V bakalářské práci se věnuji bezpečnosti v kyberprostoru a snažím se určit, zda teoretické koncepty z technologické domény jaderných zbraní lze použít k analýze kyberprostoru. Konkrétně se zaměřuji na konstruktivistickou perspektivu a teoretický rámec evoluce norem, který umožňuje analyzovat chování států na základě společných očekávání a identity v mezinárodním společenství. Normy, které tvoří standard vhodného chování, se neustále vyvíjí, a proto se zabývám též jejich životním cyklem. Dále se věnuji aplikaci tohoto teoretického rámce na jaderné zbraně a dvěma konceptům, které jej rozvíjejí: nukleárnímu tabu a nukleární deviaci. Uvádím vztah těchto konceptů k dominantnímu přístupu jaderného odstrašování, jejich výhody a nevýhody a jejich vzájemné rozdíly. Příspěvek těchto konceptů demonstruji jejich uplatněním na historických případech (ne)používání jaderných zbraní. Část věnovanou kyberprostoru zahajuji diskuzí terminologie a skutečností ve fungování kyberprostoru, které jej odlišují od ostatních domén. Na to navazuji analýzou dosavadní praxe kyber útoků a rozborem emergence norem ve třech oblastech: kontrole zbrojení, (ne)používání kyber zbraní a normativním odstrašování. Za metodologii používám případovou studii, jejíž předmětem je praxe útoků, strategie USA a mezinárodní vyjednávání. Na kyberprostor aplikuji teoretický rámec evoluce norem a teoretické přístupy z jaderné domény. V závěru se věnuji užitečnosti norem a použitých přístupů k obohacení analýzy bezpečnosti kyberprostoru.

Annotation

In my bachelor thesis I consider security in cyberspace and attempt to establish, whether theoretical approaches to the technological domain of nuclear weapons can merit the analysis of cyberspace. More specifically, I focus on the constructivist perspective and the theoretical framework of norm evolution that allows me to analyze the behavior of states based on their shared expectations and identity in international community. Norms, which form a standard of appropriate behavior, always evolve and thus I deal with their life-cycle. Further I inquire into the application of this theoretical framework in nuclear weapons and into two concepts that expand upon it: nuclear taboo and nuclear deviation. I present the relationship between these two concepts and the dominant approach of deterrence, their pros and cons, and their

differences. I demonstrate the contribution of these concepts by applying them to historical cases of (non-)use of nuclear weapons. The part of my thesis devoted to cyberspace begins with a discussion of terminology and of the aspects that differentiate cyberspace from other domains. I follow this up by a study of previous practice of cyber attacks and by the analysis of norm emergence in three areas: arms control, (non-)use of cyber weapons, and normative deterrence. My method is a case study, the object of which is the practice of attacks, cyber strategy of USA, and international negotiations. I apply the theoretical framework of norm evolution and the normative approaches from the nuclear domain to cyberspace. In the conclusion, I assess the usefulness of these approaches in enriching the analysis of cyberspace security.

Klíčová slova

Kyberprostor, normy, jaderné zbraně, kontrola zbrojení, odstrašování, případová studie, USA

Keywords

Cyberspace, norms, nuclear weapons, arms control, deterrence, case study, USA

Title

Relevance of norms in cyberspace

Poděkování

Na tomto místě bych rád poděkoval PhDr. Vítovi Stříteckému, M.Phil., Ph.D. za vedení mé práce, za čas, který mi věnoval, a za hodnotné rady, které mi poskytl.

Teze závěrečné diplomové práce

Katedra politologie IPS FSV UK

Příjmení, jméno:	Crha Miroslav				
Název práce:	Relevance norem v kyberprostoru				
Vedoucí práce:	PhDr. Vít Střítecký, M.Phil., Ph.D.	Název práce v AJ:	Relevance of norms in cyberspace		
Studijní obor:	Politologie a mezinárodní vztahy (Bc.)	Semestr zadání:	zimní		
Ak. rok podání:	2016/2017	Předpokládaný termín dokončení:	LS 2018	Typ práce:	bakalářská

Zdůvodnění výběru práce (max 2000 znaků):

K výběru tohoto tématu mě vedl zájem o nové technologie a o snahy států tyto technologie využít k prosazování svých politických a bezpečnostních cílů. Zatímco tématu informační války je věnována výrazná pozornost (například v kontextu amerických prezidentských voleb 2016), kyber útoky ve vojenském smyslu jsou dle mého názoru stále vnímány jako okrajové téma. Přitom případy jako virus Stuxnet nebo použití kyber prostředků ve válce v Jižní Osetii ukazují značný potenciál těchto prostředků ovlivnit dynamiku bezpečnostních vztahů.

Zajímají mě také normativní vlivy na rozhodování států, které sehrály velkou roli v praxi používání, respektive nepoužívání, nukleárních zbraní. Zejména jde o normativní odstrašování a o tabuizaci.

Otázka, kterou si v práci pokládám, jaký vliv mají normy v kyberprostoru, propojuje můj zájem o teoretické koncepce norem v prostředí nukleárních zbraní s realitou rozvíjejícího se kyberprostoru.

Předpokládaný cíl (max 1500 znaků):

Cílem práce je nalézt odpověď na otázku, jakým způsobem ovlivňují normy v kyberprostoru chování států. Konkrétně se budu zabývat normativním odstrašováním, tabuizací (a rozdělením na konvenční a nekonvenční zbraně) a arms control. Součástí práce bude zkoumat ze sekundárních zdrojů, jak tyto normy fungovaly a fungují v případě nukleárních zbraní. Na to naváži zkoumáním dostupných strategických dokumentů ke kyber strategiím s otázkou, zda jsou tyto strategie ovlivněny působením výše zmíněných norem, či zda je rozhodování států v kyberprostoru ovlivněno jinými normami.

Metodologie práce (max 1500 znaků):

V první části práce se budu zabývat normami v nukleárních zbraních. Budu vycházet ze sekundárních zdrojů, které se zabývají normativním odstrašováním, tabuizací a arms control. Klíčové koncepty pro tuto část budou "deterrence by denial", "deterrence by punishment", rozdělení zbraní na konvenční a nekonvenční a další koncepty vycházející z literatury odstrašování a z práce Niny Tannenwald (The Nuclear Taboo).

V druhé části se budu věnovat pokusům o aplikaci normativního odstrašování na kyberprostor, práci Tima Stevense (A Cyberwar of Ideas? Deterrence and Norms in Cyberspace) a vnímání kyperprostoru jako primárně zaměřeného na obranu.

V třetí části budu analyzovat primární zdroje, tedy strategické dokumenty ke strategii v kyberprostoru. Vzhledem k jejich dostupnosti se budu zejména zabývat strategií USA (DOD Cyber Strategy) a NATO (NATO Cooperative Cyber Defense Center of Excellence, Tallinn).

Ve čtvrté části budu porovnávat zjištění ohledně strategie z části třetí s normativními přístupy z části druhé. S normativním pohledem budu polemizovat zejména na základě rozšiřování active cyber defenses, které jsou i přes svůj název ofensivním mechanismem a, dle zjištění z třetí části, na základě vnímání vlivu norem ve strategii.

Základní charakteristika tématu (max 1500 znaků):

Kyberprostor je nejmladší a nejrychleji se rozvíjející doménou konfliktu mezi státy. Informační komunikační technologie jsou klíčovým prvkem fungování moderních států a jejich narušení může tvořit značné problémy pro národní bezpečnost. Zároveň je potřeba nevnímat kyberprostor jako izolované bojiště, protože kyber útoky mohou mít konkrétní materiální důsledky - ať už se jedná o zničení íránských centrifug v případě viru Stuxnet, nebo o vojenskou strategickou výhodu Ruska způsobenou kyber útoky na Gruzii ve válce o Jižní Osetii. Kyber si s sebou také nese závažný problém přičitatelnosti, kdy lze v mnoha případech jen těžko odhalit identitu útočníka, či zda je tento útočník státním nebo nestátním aktérem. Vzhledem k omezenému množství známých kyber útoků zatím k tématu neexistuje rozsáhlý teoretický podklad.

Z této situace vychází snaha aplikovat na kyberprostor normy původně vzniklé pro nukleární zbraně. Tato snaha je zejména přítomná v konstruktivistickém pohledu Tima Stevense, který zformuloval v roce 2012. Tento pohled předpokládá, že strategie kyberprostoru je zaměřena na defensivní opatření. Od té doby lze však vnímat významný rozvoj opatření ofensivních zvaných active cyber defenses. Označení active cyber defenses vychází ze vzdušné obrany a znamená opatření, která mají za cíl zničit nebo zredukovat efektivitu kyber hrozeb proti vlastním či spojeneckým prostředkům.

Předpokládaná struktura práce (max 1400 znaků):

Úvod

1. Normativní přístupy k nukleárním zbraním
    1.1. Normativní odstrašování, deterrence by denial, deterrence by punishment
    1.2. Tabuizace nukleárních zbraní, rozdělení na konvenční a nekonvenční zbraně, role protestů proti jaderným zbraním
    1.3. Nukleární arms control
2. Normativní přístupy v současné kyber literatuře
3. Analýza strategických dokumentů
    3.1. Strategické cíle a jejich motivace
    3.2. Kyber aktivity a kyber arzenál
    3.3. Rozvoj a směřování kyber strategií
4. Aplikace normativních přístupů na strategii
5. Závěr

Základní literatura (10 nejdůležitějších titulů):

STEVENS, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy [online]. 2012, 33(1) [cit. 2017-04-30]. DOI: 10.1080/13523260.2012.659597. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/13523260.2012.659597

TANNENWALD, Nina. The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. International Organization [online]. 1999, 53(3) [cit. 2017-04-30]. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/13523260.2012.659597

NATO Cooperative Cyber Defense Center of Excellence Tallinn, Estonia [online]. [cit. 2017-04-30]. Dostupné z: https://ccdcoe.org

The Department of Defense Cyber Strategy: April 2015 [online]. [cit. 2017-04-30]. Dostupné z: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

FREEDMAN, Lawrence. Deterrence: A reply. Journal of Strategic Studies [online]. 2006, 28(5) [cit. 2017-05-02]. DOI: 10.1080/01402390500393944. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/01402390500393944

SMETANA, Michal. JADERNÁ INFRASTRUKTURA VE SVĚTĚ BEZ JADERNÝCH ZBRANÍ: Logika virtuálních arzenálů v kontextu jaderného odzbrojení. Obrana a strategie (Defence and Strategy) [online]. 2015, 15(1) [cit. 2017-05-02]. DOI: 10.3849/1802-7199.15.2015.01.019-030. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2015/1-2015/clanky/jaderna-infrastruktura-ve-svete-bez-jadernych-zbrani.html

Obsah

Úvod

Ve své bakalářské práci jsem se rozhodl zabývat kyberprostorem, protože jej považuji za fascinující novou technologickou doménu, ale zároveň protože jsem názoru, že chápání bezpečnosti v kyberprostoru výrazně zaostává za jeho rapidním technologickým vývojem. Mým zájmem je prozkoumat, zda teorie a koncepty, které úspěšně vysvětlují chování států v doméně jaderných zbraní, mohou fungovat jako efektivní analytické nástroje v kyberprostoru. Samotné jaderné zbraně byly v polovině 20. století technologickou inovací, jejíž význam a fungování bylo potřeba vysvětlit kombinací již zavedených a zcela nových přístupů. Poznatky vyplývající z více než 70 let zkoumání jaderných zbraní pomáhají porozumět chování států, když reagují na technologickou změnu, která ovlivňuje otázky národní bezpečnosti. V této práci však nemám ambici aplikovat rozsáhlý korpus teorie týkající se jaderných zbraní ve svém celku na kyberprostor – to by vydalo na mnoho monografií. Budu se specificky věnovat konstruktivistickému přístupu k normám. Normy jako nukleární tabu pomohly vysvětlit chování států v situacích, kdy dominantní přístup odstrašování nepostačoval. Jejich přínosem je rozšíření čistě materiální perspektivy, která se soustředí na strategickou výhodnost použití (jaderných) zbraní o faktory spojené se vzájemnými vztahy států, sdílenými očekáváními a identitou v mezinárodním společenství. Normy určují vhodné chování aktérů a důsledky plynoucí z odchýlení se od tohoto chování. Nejde však o neměnný fenomén – a právě proto je považuji za vhodné pro zkoumání jak jaderných zbraní s dekádami praxe a výzkumu, tak relativně nového prostředí kyber zbraní. Normy procházejí evolucí, kdy v různých stádiích ovlivňují chování států rozdílnými mechanismy s rozdílnými důsledky při jejich porušení.

Pokládám si tedy výzkumnou otázku, zda normativní přístupy k jaderným zbraním mohou fungovat jako efektivní analytické nástroje v kyberprostoru. Zodpovězení této otázky vyžaduje několik kroků. Prvním je uvedení teoretického rámce evoluce norem. Druhým krokem je nalézt, jak je tento rámec specifikován a používán kontextu jaderných zbraní. A posledním a nejdůležitějším krokem je pokusit se tyto poznatky aplikovat na kyberprostor. Úspěšnost uplatnění tohoto přístupu v kyberprostoru mi umožní učinit závěr ohledně užitečnosti získaných poznatků v analýze této nové domény. Těmto krokům v zásadě odpovídá struktura práce, pouze mezi první a druhou část je vložena část o metodologii. Obsahově tyto kroky odpovídají projektu bakalářské práce, ale strukturu uvedenou v projektu jsem pozměnil

v zájmu logičtějšího a lépe srozumitelného postupu od obecné teorie přes její specifické použití k aplikaci na novou doménu.

Za metodologii práce jsem zvolil případovou studii. Ačkoliv lze evoluci norem zkoumat i kvantitativními metodami, ty se soustředí na konkrétní bod vývoje předem známé normy, například dosažení přelomového bodu ve stádiu síření normy. Kvalitativní výzkum mi umožní věnovat se i méně prozkoumaným normám v kyberprostoru, jejichž stádium vývoje není předem známé. Dostupnost informací o uvažování a chování států v kyberprostoru se navíc výrazně liší mezi jednotlivými státy, což umožňuje hlubokou analýzu pouze v některých případech. Subjektem mé případové studie je tedy test aplikovatelnosti normativních přístupů k jaderným zbraním na kyberprostor a předmětem je dosavadní praxe kyber útoků, strategická literatura USA a vyjednávací pozice států na mezinárodních platformách.

Samotným normám se budu věnovat ve třech oblastech. Zaprvé to je kontrola zbrojení a odzbrojování. Zadruhé jde o (ne)používání zbraní. Zatřetí se budu zabývat vztahem norem a odstrašování. Z literatury k jaderným zbraním jsem zvolil dva normativní přístupy: nukleární tabu a nukleární deviaci. Tyto přístupy se od sebe významně liší a díky tomu se komplementují – zatímco nukleární tabu lépe prokazuje působení normy a určuje stádium jejího vývoje, nukleární deviace zdůrazňuje plynulý vývoj a vzájemnou interakci norem.

Práce je rozdělena do čtyř částí. V první části zabývající se teoretickým rámcem evoluce norem se pokusím definovat normy, jejich význam, jejich důsledky a následky jejich porušování. Poté uvedu životní cyklus norem, jednotlivá stádia životního cyklu, mechanismy, kterými jsou normy ovlivňovány a ovlivňují státy, a vývoj nutný k posunutí do dalšího stádia. V druhé části uvedu metodologii, dle které v této práci postupuji. V třetí části představím terminologii kontroly zbrojení a souvisejících pojmů, historii jaderného zbrojení a normativní koncepty v jaderném zbrojení včetně jejich vztahu k odstrašování. Fungování těchto konceptů se pokusím demonstrovat na historických případech (ne)používání jaderných zbraní. Ve čtvrté a nejdůležitější části začnu terminologií kyberprostoru a specifickými podmínkami kyberprostoru, kterými se liší od ostatních domén. Poté se pokusím analyzovat dosavadní praxi kyber útoků a zda z ní jde vyčíst vliv norem. Na to navážu zkoumáním kontroly kyber zbrojení, kyber (ne)útočením a normativním odstrašováním a v každé z těchto oblastí se budu snažit odhalit, zda dochází k emergenci určitých norem. V závěru zhodnotím úspěšnost použitých analytických nástrojů v kyberprostoru.

1 Teoretický rámec

Za teoretický rámec své práce jsem zvolil konstruktivistický přístup vycházející z Finnemore a Sikkink (1998). Tento přístup umožňuje zkoumat odpovědi na následující otázky: jak poznat normu, jaké důsledky mají normy v politice, odkud normy pocházejí. Klíčovou výhodou je ale zejména schopnost vysvětlit evoluci norem a jejich životní cyklus. Kyberprostor, který je tématem této práce, je relativně mladým vynálezem a proto vyžaduje přístup, který se více než na stabilní a rozvinuté normy soustředí na jejich vývoj od emergence přes rozšíření po internalizaci. Určení, ve kterém životním stádiu se norma nachází, mi umožní zjistit, jakým vlivem a jakou silou působí na chování států a znalost vztahu mezi jednotlivými stádii pomůže formulovat očekávání ohledně budoucího vývoje norem.

„*Existuje obecná shoda na definici normy jako standardu vhodného chování pro aktéry s určitou identitou*“ (Finnemore a Sikkink 1998, s. 891). Dále je však třeba definovat – a určit vztah mezi – některými souvisejícími termíny. Na rozdíl od izolovaného a konkrétního chování upraveného normou, pojem instituce chápu jako sadu více souvisejících norem. Efekty norem lze dále dělit na 1) regulativní, které nařizují a omezují chování, 2) konstitutivní, které vytváří nové aktéry, zájmy a kategorie, a 3) preskriptivní, které určují, jaké chování je žádoucí. Pro zkoumání norem je důležité určit komunitu, ve které se konkrétní norma vyskytuje. Příslušnost ke komunitě navíc často nelze určit binárně, může se mezi jednotlivými aktéry lišit svou intenzitou. Ve studiu norem v mezinárodních vztazích typicky za komunitu považujeme mezinárodní společenství tvořené státy (Finnemore a Sikkink 1998, s. 892).

1.2 Životní cyklus norem

Vliv sdílených představ a očekávání, které jsou v konstruktivistickém pojetí nutnou součástí prostředí, ve kterém pozorujeme normy, pomáhá vysvětlit normativní stabilitu, ale je podstatně méně úspěšný při výzkumu změny. Tyto představy a očekávání totiž nejsou neměnné a prochází různými vývojovými stádii. V každém stádiu jsou představy a očekávání aktérů ovlivňovány jinými mechanismy a také jinak působí na vnímání norem a identity. Právě rozpracování těchto stádií a jejich mechanismů považuji za hlavní přínos zvolené teorie. Finnemore a Sikkink (1998, s. 895) uvádí tři stádia životního cyklu norem: emergenci, kaskádu a internalizaci.

1.2.1 Emergence

V prvním stádiu, emergenci, dochází k přesvědčování ze strany ‚norm entrepreneurs'. Tito ‚podnikatelé s normami' vychází z přesvědčení o vhodnosti určitého chování a prostřednictvím jazyka vytvářejí a spravují významy a aplikují je na různá témata[1]. Při tomto procesu však nevstupují do prázdného prostoru, ale soutěží s normami, které zde již existovaly dřív. V tomto stádiu životního cyklu normy v mezinárodních vztazích je důležitý i její vztah k souvisejícím domácím normám. Tento proces vzájemného ovlivňování domácích a mezinárodních norem je dobře pozorovatelný na příkladu volebního práva žen. To bylo původně domácím požadavkem v některých státech, ale postupným rozšiřováním této myšlenky došlo k přelomovému bodu, kdy tento požadavek díky svému rozšíření začal působit normativně i na mezinárodní úrovni. Tuto mezinárodní normu potom mohou použít norm entrepreneurs v domácím kontextu k posílení své menšinové pozice (Finnemore a Sikkink 1998, s. 893).

Posun z prvního do druhého stádia životního cyklu normy nastává překročením určitého prahu. Jakmile dojde k dostatečnému rozšíření normy, hlavní mechanikou jejího dalšího rozšiřování již není přesvědčování, ale přizpůsobování se. Kdy konkrétně nastalo překročení prahu u dané normy bývá tématem kvantitativních empirických výzkumů, není však rozvinutý teoretický rámec, který by umožňoval apriorně určit, kdy, kde a jak lze překročení prahu očekávat (Finnemore a Sikkink 1998, s. 901). Pro mnoho norem tato změna nastává jejich institucionalizací v mezinárodních organizacích a mezinárodních smlouvách. Nejedná se však o nutnou podmínku – zdaleka všechny normy nejsou podloženy mezinárodním právem a značná část těch, které jsou, vychází z obyčejového práva, které takto institucionalizované není[2]. Institucionalizace též může nastat později v druhém stádiu životního cyklu. Překročení prahu může též urychlit adopce normy určitými klíčovými státy. Které státy lze považovat za klíčové se liší případ od případu, zpravidla však za klíčový lze považovat stát, který pokud normu neadoptuje, ohrozí její cíl. V případě jaderného odzbrojení tedy klíčové budou zejména státy, které jaderné zbraně vlastní.

[1] Tímto procesem se zabývají i další disciplíny – právní teoretik Lessig (1995) používá pojem manažer významu, zatímco v sociologii se používá související koncept rámování (framing). Specifickým případem z prostředí bezpečnostních studií může být i koncept sekuritizace.

[2] Paradoxně k institucionalizaci může dojít praxí – pokud jej použije některý z mezinárodních soudů ve svém rozhodnutí. Ve sporech o existenci obyčejového pravidla jde z perspektivy norem o rozdílný názor dvou aktérů na to, zda se cítí být zavázáni určitou normou. Příkladem může být rozsudek MSD z roku 1960 v případě práva přechodu přes indické území (Portugalsko v. Indie).

1.2.2 Kaskáda

Druhým stádiem životního cyklu normy je kaskáda. Zatímco v prvním stádiu bylo důležité přesvědčování ze strany norm entrepreneurs a existence vnitrostátních platforem, které se snaží normu prosadit, po dosažení prahu začnou další státy přijímat normu rychlejším tempem, aniž by je k tomu nutily domácí tlaky. Tento nový mechanismus vzniká ve vztazích mezi státy, kde je vyvíjen tlak na porušovatele normy, aby ji začali respektovat. Motivací pro přizpůsobení se normě může být legitimizace státu a snaha vyhnout se označení za ničemný stát (rogue state), což vede k poškození reputace a důvěryhodnosti státu – a to nejen v mezinárodním společenství, ale i z hlediska vnímání legitimity státu jeho občany (Finnemore a Sikkink 1998, s. 903). Další motivací je konformita, jejíž význam podporuje koncept „social proof". Nejen, že usuzujeme vhodnost chování podle toho, zda vidíme ostatní se tak chovat, také to ovlivňuje názory na to, jak se nejlépe přizpůsobit sociálnímu prostředí (Axelrod 1986, s. 1005). Jinými slovy: státy se podřizují normám, aby dokázaly, že jsou ochotny přizpůsobit se a být tak součástí mezinárodního společenství. Soulad s pravidly a sounáležitost s mezinárodním společenstvím též ovlivňují, jak státy vnímají vlastní identitu, ale též i jak jedinci, kteří v rámci státu určují jeho chování v mezinárodní aréně, vnímají svoji identitu. Tyto vedoucí osoby v důležitých státních institucích bývají často cílem kritiky ze strany norm entrepreneurs a mohou prožívat kognitivní disonanci, stav nepříjemného nesouladu mezi vnímáním svých hodnot a svého chování (Finnemore a Sikkink 1998, s. 905).

1.2.3 Internalizace

Důsledkem druhého stádia je široké rozšíření normy jako standardu vhodného chování. To však neznamená, že se s ní státy automaticky ztotožní – některé státy kupříkladu normu dodržují, protože se bojí ztráty legitimity či důvěryhodnosti, ale nejsou vnitřně přesvědčeny o její správnosti. Dodržování normy nepovažují za samozřejmost, o které ani není potřeba diskutovat. Právě tato kvalita se mění internalizací normy. Chování postulované internalizovanou normou provádíme automaticky a nepovažujeme jej za kontroverzní. Internalizované normy jsou proto nejen velmi silné, ale také v politice špatně rozpoznatelné, protože nejsou tématem, o kterém by se diskutovalo.[3] Internalizace probíhá několika procesy, které spolu na první pohled nemusí souviset. Určitá zaujatost vzniká odborným vzděláním a

[3] V sociologii, na rozdíl od politologie, je internalizovaným normám věnována značná pozornost. Důvodem může být, že zatímco politologie se častěji věnuje snaze vysvětlit rozdíly v chování mezi státy, sociologie se zabývá společnými znaky.

přípravou v určitých profesích, jako je třeba ekonomická nebo právnická (Finnemore a Sikkink 1998, s. 904-905). Nerovnoměrné zastoupení těchto profesí v rozhodujících institucích může jednostranně směřovat vnímání normy v rámci státu. Opakování určitého chování a zvyk může vést k jeho postupnému přijetí za automatické. S tím pracuje neofunkcionalismus ve studiu evropské integrace. Ernst B. Haas „*posunul zájem výzkumu […] k důležitosti organizovaných zájmových skupin a k roli, kterou jejich dynamická interakce může hrát při vytváření důsledků integrace*“ (Rosamond 2005, s. 241). Jinými slovy, častá interakce a spolupráce vede ke zvyku a internalizaci důvěry mezi účastníky.

2 Metodologie

Za metodu této bakalářské práce jsem zvolil případovou studii. Cílem je otestovat, zda normativní koncepty úspěšné v jaderné technologické doméně mohou jako analytické nástroje obohatit výzkum kyberprostoru. Toho dosáhnu použitím těchto nástrojů ve zkoumání, zda aktéři, kterými jsou státy, již uznávají v kyberprostoru určité normy a případně v jakém jsou stádiu vývoje. Proto se budu zabývat rozborem teoretických konceptů norem, které fungují v kontrole jaderného zbrojení, nepoužívání jaderných zbraní a v jaderném odstrašování a pokusím se aplikovat tyto koncepty na kyberprostor. Část o kyberprostoru zahájím analýzou nedávných útoků v kyberprostoru. V případě, že z praxe nedávných útoků nebude možné dojít k závěru, že se státy již cítí být vázány nějakou normou, budu zkoumat emergenci norem. To provedu analýzou relevantních strategických, diplomatických, právních i jiných zdrojů. Soustředit se budu na strategii USA, protože jde o zemi s velkými schopnostmi v kyberprostoru, ale i závislostí na něm, a protože na rozdíl od ostatních kyber velmocí jsou její strategické dokumenty často veřejně dostupné. Přístup ostatních zemí budu sledovat skrze vyjednávání na mezinárodních platformách, jako je OSN nebo série konferencí tzv. Londýnského procesu. Pokusím se identifikovat některé „kandidátní“ normy a na základě hypotéz založených na historické zkušenosti s vývojem norem u nových technologií se pokusím určit, zda je pravděpodobné, že emergence bude úspěšná (tj. zda se podaří překročit práh pro kaskádu).

3 Kontrola jaderného zbrojení

3.1 Úvod a terminologie

V této části se budu věnovat historickému a teoretickému vývoji norem v jaderné technologické doméně. Budu se zabývat normami kontroly jaderného zbrojení a jaderného odzbrojení, (ne)používání jaderných zbraní a jak mohou normy obohatit koncept jaderného odstrašování. Na rozdíl od kyberprostoru je problematika jaderných zbraní déletrvající a nabízí rozsáhlejší a hlubší literaturu. Teoretické koncepty, které vycházejí z aplikace rámce evoluce norem na jaderné zbrojení, úspěšně vysvětlují některé fenomény, které tradičnější přístupy jako odstrašování vysvětlit nedokáží. Cílem této části je uvést, vysvětlit a demonstrovat na historických případech silné a slabé stránky těchto konceptů v rámci širší snahy zjistit, zda normativní přístup může být vhodným analytickým nástrojem pro zkoumání kyberprostoru. Za tímto účelem se budu věnovat dvěma konceptům – jadernému tabu a jaderné deviaci – pomocí kterých budu sledovat vývoj norem od druhé světové války.

Prvním krokem je vymezení některých pojmů. Odzbrojování (disarmament) je „*proces snižování stavu ozbrojených sil a vojenských výdajů, zničení nebo odstranění zbraní, ať rozmístěných nebo skladovaných, postupná likvidace kapacity vyrábět nové zbraně, uvolnění a zařazení vojenského personálu do civilního života*“ a kontrola zbrojení „*opatření, která kvalitativně anebo kvantitativně omezují nárůst počtu, resp. ničivé síly (jaderných) zbraní a případě regulaci dalších činností spojených s těmito zbraněmi*“ (Bříza 2010, s. 22-23). Na základě těchto definicí považuji odzbrojování za ambicióznější cíl vyžadující snížení stavu zbraní a též za podskupinu šířeji definovaných opatření kontroly zbrojení, které cílí zejména na omezení nárůstu počtu a síly zbraní. Toto rozdělení je však primárně teoretické a neshoduje se s používáním těchto pojmů v OSN, kde je odzbrojení používáno za obecnější a širší termín (Bříza 2010, s. 23-24). Terminologie zde použitá reflektuje záměr zkoumat obecnější normu kontroly zbrojení a její vývoj s tím, že odzbrojení považuji za intenzivnější formu této normy.

3.2 Historie kontroly jaderného zbrojení

První snahy o kontrolu jaderného zbrojení nastávají bezprostředně po prvním použití jaderných zbraní. Toto téma se stalo jedním z hlavních úkolů stojících před nově vzniklým OSN

a první významný plán přišel, poněkud překvapivě, z USA[4], tedy jediného státu, který jadernou zbraň použil. Takzvaný Baruchův plán navrhoval zřízení mezinárodního Úřadu pro jaderný rozvoj, který by měl pravomoc absolutní kontroly nad světovými zásobami uranu a thoria. Cílem bylo mírové poskytování vědeckých poznatků a úplná eliminace nukleárních zbraní s širokým kontrolním aparátem (Baruch 1946). Zatímco tento a další plány z druhé poloviny 40. let prezentovaly utopické požadavky, které byly pro některé státy nepřijatelné, zlom nastal v roce 1949, kdy Sovětský svaz provedl první úspěšný test jaderné zbraně. USA tím ztrácí značnou výhodu a následují 50. léta rapidního zbrojení a testů stále silnějších zbraní (Bříza 2010, s. 30). Z hlediska bezpečnosti sice mohlo jít o postupné dosažení rovnováhy mezi americkým a sovětským jaderným arsenálem, z hlediska norem a kontroly zbrojení je však zřejmé, že k (pozitivnímu) vývoji nedochází. Přesto lze i v 50. letech pozorovat snahy o přechod k mírovému využití jaderných technologií, tyto snahy však narážely na vzájemnou nedůvěru v bipolárním systému, což je zřejmé například z projevu Atoms for Peace amerického prezidenta Eisenhowera: „*Ale hrozivé tajemství a strašné stroje jaderné síly nejsou jen naše. Jednak toto tajemství drží i naši přátelé a spojenci Velká Británie a Kanada, jejichž geniální vědci významně přispěli našim původním objevům v návrhu jaderných zbraní. Toto tajemství také zná Sovětský svaz*“ (Eisenhower 1953, s. 3). V této vlivné řeči, která vedla mimo jiné k založení Mezinárodní agentury pro atomovou energii (IAEA), dále Eisenhower zmiňuje, že schopnost USA odpovědět na jaderný útok je „*tak velká, že by země protivníka lehla popelem – a to ačkoliv by nešlo o pravé vyjádření smyslu a nadějí Spojených států.*“

Kromě velmi dílčích úspěchů jako již zmíněné založení IAEA a snahy omezit určité typy jaderných testů však jednání selhávala. Potřebnou, ač hrozivou, novou perspektivu poskytla až kubánská raketová krize v roce 1962 a s ní spojené bezprostřední riziko propuknutí jaderné války. Přestože se krizi podařilo zažehnat, její vliv na vnímání jaderného rizika byl trvající (Bříza 2010, s. 31).

[4] Zde je potřeba zmínit jeden aspekt fungování norem, který zmiňuje i Finnemore a Sikkink (1998). V krizových situacích, kdy porušení normy může vést k velmi pozitivním důsledkům pro některé státy, může docházet k velmi rychlému zhroucení norem. Ve druhé světové válce se takto například zhroutila norma zakazující kobercové bombardování. Poválečný přístup USA k používání jaderných zbraní může být vnímán jako podobný příklad, kdy materiální prospěch převážil sílu normy – nedá se však ještě hovořit o normě nepoužívání jaderných zbraní, ale spíše o šířeji nelegitimní útok nerozlišující mezi civilními a vojenskými cíli, zvlášť vzhledem k rozsahu.

Po kubánské raketové krizi se dostavily první úspěchy. V roce 1963 byla uzavřena smlouva PTBT, která zakazuje určité typy testů jaderných zbraní. Již název Partial Nuclear Test Ban Treaty však naznačuje, že finální text smlouvy nedokázal naplnit veškerá očekávání. Důvodem byly opět zejména technické náležitosti spojené s kontrolou dodržování a neochota Sovětů na ně přistoupit (Bříza 2010, s.31). Dalším úspěchem 60. let byla Smlouva z Tlatelolco, která zakazuje testování, výrobu, získávání a použití jaderných zbraní v Jižní Americe a Karibiku[5]. Nejdůležitější smlouvou tohoto období je smlouva o nešíření jaderných zbraní (NPT) z roku 1968. Tato smlouva, která zavazuje nejaderné státy, aby neusilovaly o získávání jaderných zbraní, a jaderné státy, aby postupně odzbrojovaly, je dodnes jedním z nejefektivnějších nástrojů kontroly jaderného zbrojení. A to i přes její slabinu v plnění závazku jaderných států odzbrojovat (Bříza 2010, s. 32).

70. léta byla specifická uvolněním vztahů mezi USA a SSSR a návratem k bilaterálním jednáním, které vedly ke snížení počtu nosičů a dosažení parity jaderných zbraní ve smlouvách SALT I a SALT II[6]. Ostatní návrhy nadále ztroskotávaly kvůli rozdílným vizím dlouhodobých cílů kontroly jaderného zbrojení (Adler 1992, s. 103), které se projevovaly v sovětské neochotě přistoupit na inspekce na místě a americké neochotě uzavírat smlouvy bez efektivních mechanismů pro ověření dodržování.

Důležitý přelom tak nastává až v polovině 80. let, kdy se ekonomické problémy Sovětského svazu vyžadující omezení výdajů na zbrojení a přístup Michaila Gorbačova zasloužily o ustoupení sovětů a jejich ochotu přistoupit na inspekce na místě. Výsledkem byla smlouva INF z roku 1987 o likvidaci raket středního a kratšího doletu a START I požadující snížení počtu strategických jaderných zbraní z roku 1991. Z hlediska mezinárodního práva jsou obě smlouvy přelomové svým komplexním kontrolním mechanismem (Bříza 2010, s. 35). Po rozpadu Sovětského svazu se pokrok dále urychlil, když se bývalé státy SSSR dobrovolně staly nejadernými státy a byla podepsána smlouva o úplném zákazu jaderných zkoušek CTBT.

[5] Tímto vzniká první zóna bez jaderných zbraní. Další taková zóna vznikla až v roce 1986, dnes však tyto zóny pokrývají prakticky celou jižní polokouli. Do tohoto shrnutí záměrně nezahrnuji Kosmickou smlouvu, Smlouvu o Antarktidě a Smlouvu o mořském dně, ačkoliv jejich režimy de facto vytvářejí zóny bez jaderných zbraní.
[6] Jednání o SALT II trvala až do roku 1979, sporem byly opět kontrolní mechanismy. Mezi podpisem a ratifikací smlouvy však proběhla sovětská invaze do Afghánistánu a USA ji následně odmítla ratifikovat; „obě země se však víceméně chovaly v souladu s jejími ustanoveními“ (Bříza 2010, s. 32).

Druhá polovina 90. let a následný vývoj znamenal zpomalení kontroly jaderného zbrojení a v některých ohledech dokonce krok zpět. Americký senát odmítl ratifikovat smlouvu CTBT. START II, která měla navázat na úspěchy i komplexní řešení START I, se nedařilo ratifikovat v Rusku. START II definitivně neuspěla v roce 2002[7], kdy USA dokonce odstoupila od smlouvy ABM vyjednané v rámci rozhovorů SALT I. Navíc po konci bilaterálního uspořádání studené války dochází k další vlně proliferace jaderných zbraní, které se podařilo vyvinout Pákistánu, Indii a Severní Koreji (Bříza 2010, s. 33-35)

3.3 Normativní přístup ke kontrole jaderného zbrojení

Předchozí shrnutí historického vývoje snah o kontrolu jaderného zbrojení přistupuje k chování států čistě popisně. Lze z něj tedy vypozorovat několik tendencí, pro jejichž vysvětlení však bude potřeba použít jiného přístupu, za který jsem zvolil normy. Tyto tendence se mohou jevit jako očividné, nicméně se domnívám, že za tím může stát retrospektivní pohled a síla norem působících na naše vnímání těchto chování. Jednak zde existuje velmi silná tendence jaderné zbraně nepoužívat. Kromě Nagasaki a Hirošimy nikdy k použití nedošlo a oba dva útoky proběhly bezprostředně po vyvinutí jaderných zbraní prvním státem. Nepochybně lze nalézt konkrétní situace, kdy se tak nestalo jen díky štěstí nebo mimořádným schopnostem jedinců, kteří čelili planým poplachům, přesto se však jedná o velmi silný trend, který nelze zjednodušit na vysvětlení pouze úvahami realistů o odstrašování a vzájemně zaručeném zničení, čemuž se budu dále věnovat. Další tendencí je, že jednání o omezení jaderných zbraní často selhávaly z praktických a technických důvodů nedůvěry a problematičnosti systémů pro ověřování dodržování smluv, přesto lze však vidět vůli a snahu pokračovat ve vyjednáváních a snížit množství a možnosti použití „strašných zdrojů jaderné síly“. Z vyjadřování klíčových aktérů vyplývá, že kontrola jaderných zbraní je jednoznačně morální řešení. Co se týče vztahu mezi národními zájmy a jadernými zbraněmi, zde bude důležité vrátit se k rámování a roli norm entrepreneurs – aktéři, kteří normu prosazují, nejednají proti svým vlastním zájmům, ale jednají v souladu s novým rámcem chápání těchto svých zájmů. Změny v chápání role jaderných zbraní jakožto součásti bezpečnostní politiky státu tedy budou silným indikátorem působení norem.

[7] Jako náhrada za START II byla přijata smlouva SORT, podle které musí Rusko i USA výrazně snížit svůj počet jaderných hlavic, chybí zde však kontrolní systém obdobný START I nebo návrhu START II.

Velmi oblíbeným teoretickým konceptem pro zkoumání motivace států ve vlastnění a používání jaderných zbraní je odstrašování (deterrence)[8]. Tento koncept, který vysvětluje, proč státy (ne)vlastní a (ne)používají jaderné zbraně však předpokládá chování, které v některých případech neodpovídá realitě, například nedokáže vysvětlit „*V prvních zhruba deseti letech studené války, kdy Spojené státy držely absolutní jaderný monopol, […] americké ne-použití ve Vietnamu, […] proč Británie nepoužila jaderné zbraně na Falklandech, ani proč Sovětský svaz nevyužil jaderné zbraně k odvrácení porážky v Afghanistánu*“ (Tannenwald 1999, s. 434). V rozporu s konceptem odstrašování však nejsou jen případy, kdy jaderné státy odmítly zbraň použít, ale též případy, kdy došlo k útoku (a tedy ne k odstrašení) nejaderných států na jaderné státy[9]. Dle konceptu odstrašování bychom také mohli předpokládat, že nejaderné státy budou více usilovat o získání jaderných zbraní.

Tyto mezery v konceptu odstrašování se pokouší vyplnit normativní přístup nukleárního tabu[10] Niny Tannenwaldové. Existence silné normy tabuizující jaderné zbraně jako nelegitimní a nekonvenční zbraně hromadného ničení dokáže ovlivnit uvažování států jak v případech úvah nad použitím, tak také v hodnocení rizika, že bude zbraň použita proti nim. Tento posun ve vnímání užitku i rizik s jadernými zbraněmi spojenými může též obohatit realistickou perspektivu odstrašování, která je čistě materialistická, o další faktory ovlivňující předpoklady a efektivitu odstrašování.

Tannenwaldová pracuje s třemi efekty normy (regulativní, konstitutivní, permisivní), které jsem již uvedl v teoretické části. Hlavním regulativním efektem nukleárního tabu je zákaz použít jadernou zbraň jako první. Konstitutivních efektů je více – tabu určuje vnímání jaderných zbraní jako nepřijatelných zbraní hromadného ničení a na základě toho vytváří kategorii „civilizovaných“ států. Permisivní efekty jsou méně viditelné a vyplývají z fungování normy, konkrétně jejích konstitutivních efektů. V tomto případě to může být například vnímání jiných zbraní jako konvenčních a tedy legitimních (Tannenwald 1999, s. 437).

[8] Akademická vyhledávací služba Google Scholar nabízí na dotaz „nuclear deterrence“ přibližně 31 800 výsledků. Pro porovnání „nuclear taboo“, normativní přístup, kterému se zde dále věnuji, generuje pouze 2050 výsledků.

[9] Například válka v Koreji, nebo již zmíněný Vietnam a Falklandy.

[10] Slovo tabu, ač používané i jinými autory, nepopisuje přesně podstatu normy delegitimizující jaderné zbraně. Tabu označuje věci, které jsou společensky považované za nemyslitelné, o kterých se ani nemluví. To by implikovalo, že se jedná o internalizovanou normu. Jak v práci Tannenwaldové tak i v této je však tento termín vztahován k normě jako takové ve všech stádiích vývoje.

Co se týče prokazování existence a vlivu normy, Tannenwaldová rozlišuje dva typy nikoliv nepodobné kaskádě a internalizaci. V prvním případě norma vstupuje do uvažování o nákladech a přínosech určitého chování. To odpovídá delegitimizaci a ztrátě důvěry vůči státu v situaci, kdy poruší rozšířenou normu, a zároveň jde o situaci, kdy o výhodnosti jejího porušení vážně uvažuje, tedy nejde o internalizovanou normu. Druhý typ projevů normy je založen na vnímání vhodnosti určitého chování nezávisle na materiálních faktorech. Tento typ, blízký internalizované normě, autorka přirovnává k ius cogens v mezinárodním právu (Tannenwald 1999, s. 440). Toto přirovnání je poněkud problematické, protože kogentní mezinárodní právo, byť závazné pro všechny subjekty[11], bývá v praxi porušováno, pokud to dotyčnému státu přinese velkou materiální výhodou. Příkladem může být klíčový princip zákazu agrese ukotvený v článku 2 odstavci 4 charty OSN (United Nations 1945). Zároveň je však třeba uznat, že ius cogens je nejsilnějším nástrojem pro vyjádření závaznosti normy dostupný mezinárodnímu právu. Proto se domnívám, že jde o užitečný důkaz rozšíření a míry institucionalizace normy, nikoliv však dostatečný pro konstatování její internalizace.

Nukleární tabu ale není jediným normativním přístupem k jadernému zbrojení. Alternativou může být například koncept nukleární deviace vycházející z proudu symbolického interakcionismu v sociologii. Tento přístup vnímá stigma (např. označení za ničemný stát) jako intersubjektivní proces, kdy se stigmatizovaný svou reakcí podílí na významu stigmatu. Stigma také slouží jako hranice, která v kontrastu vymezuje normální chování (Smetana 2016). Tento koncept tedy dokáže lépe vysvětlit rozpad norem, protože nevnímá porušení normy jako izolovaný případ vedoucí k jednostrannému označení za nedůvěryhodného jako v případě tabu, ale jako součást neustále probíhající soutěže o normu a o posunutí hranice mezi normálním a deviantním: „*Tato perspektiva mi umožňuje ukázat, jak se chápání ‚dobrého' a ‚špatného' chování v jaderném pořádku mění v čase; a jak určité chování, zvyky a diskurzy, které by dříve mohly být považovány za normální, se stávají rozporuplnými a postupně stigmatizovanými*" (Smetana 2016; 28). Na rozdíl od teorie evoluce norem tento přístup nerozlišuje konkrétní stupně vývoje normy, což ale neznamená, že s vývojem normy nepracuje: jde zde o zcela plynulý proces. Ten se projevuje jednak v chování, které norma určuje – například NPT povoluje jen několika státům držet jaderné zbraně a porušovatelé se

[11] Tj. státy, v omezené formě též mezinárodní organizace a subjekty *sui generis* (např. Mezinárodní výbor červeného kříže).

snaží o rozšíření tohoto seznamu o sebe, ne nutně o jeho zrušení[12] – ale také v síle stigmatu, které je spojené s porušením normy. Ačkoliv tato větší flexibilita nukleární deviace oproti nukleárnímu tabu může být v některých případech výhodou, nenabízí tak přehlednou kategorizaci výsledků a nepracuje s možností internalizace normy.

3.4 Projevy tabuizace v historických příkladech

V předchozí části jsem představil dva koncepty, pomocí kterých lze analyzovat normy, jejich vliv v rozhodovacích procesech států a důsledky, které může mít porušení těchto norem. Na to navazuji využitím těchto poznatků při sledování amerického rozhodovacího procesu a vývoji jeho přístupu k možnosti použití jaderné zbraně. Ve volbě těchto příkladů následuji práci Tannenwaldové, protože mi to umožňuje sledovat, jak sama autorka svou teorii aplikuje. Tento přístup se pokusím obohatit o konstruktivistický teoretický rámec z první části této práce (Tannenwaldová se soustředí zejména na racionalistický přístup k normám), o nukleární deviaci a o primární zdroje. Příklady, kterým se tedy budu věnovat jsou: Japonsko 1945, válka v Koreji, a válka ve Vietnamu[13].

Rok 1945 byl vrcholem období rozpadu norem. Mnohé těžce vyjednané požadavky mezinárodního humanitárního práva byly porušeny a – v souladu s nukleární deviací – porušování principů proporcionality a rozlišování vojenských a civilních cílů vedlo k považování chování, které by bylo před válkou bráno za deviantní, za normální. Z norem přijatých v meziválečném období: 1) zákaz útoku ponorkami na obchodní lodě začal být porušován téměř od začátku války, 2) zákaz bombardování civilních cílů vydržel několik měsíců, ale poté začal být též porušován, a 3) zákaz chemických zbraní vydržel celou válku (Legro 1997, s. 32). Tyto tři případy ilustrují postupnou změnu hranice mezi deviantním a normálním chováním v případě humanitárních norem nutnosti, proporcionality a rozlišování (mezi civilními a vojenskými cíly). V této situaci, spolu s absencí jakéhokoliv specifického vnímání jaderných zbraní, byla jaderná zbraň pouze nejmodernější a nejsilnější bombou. Proto její použití americký prezident Truman oslavuje jako vědecký a technologický úspěch: „*Je to jaderná bomba. V ní je spoutána základní síla světa. Síla, ze které slunce čerpá svou energii, byla*

[12] Konkrétním případem může být Indie, která se odmítla připojit k NPT jako nejaderný stát a testovala jaderné zbraně. Na následnou stigmatizaci reaguje označováním NPT za diskriminační, což lze vnímat jako snahu nikoliv rozbít normu proti proliferaci, ale o rozšíření uznaných jaderných států o sebe samou. (Smetana 2016).

[13] Tannenwaldová se kromě těchto tří věnuje i válce v zálivu 1991, tu jsem se ale rozhodl do této práce nezahrnout. To z přesvědčení, že předchozí tři případy dostatečně zachycují vývoj normy a protože ke každému z těchto příkladů existuje ohromné množství literatury, kterou v této práci rozhodně nemám prostor shrnout.

uvolněna proti těm, kteří rozpoutali válku na Dálném východě“ (Truman 1945). Zároveň je nutné přiznat, že v tomto případě dochází přístup odstrašování ke stejnému závěru; Truman dodává: „*Mám pochybnosti, že taková kombinace [vědy, technologie a průmyslu] by se mohla dát dohromady kdekoliv jinde ve světě. To, co jsme dokázali, je největší úspěch organizované vědy v historii.*“ Absolutní monopol a výhled na jeho zachování zjevně eliminuje jakoukoliv možnost vzájemného odstrašování. Z hlediska norem i odstrašování jde tedy o situaci, kdy použití jaderných zbraní nebránilo nic než obecné a válkou oslabené humanitární požadavky.

Válka v Koreji byla jiná. Sovětský svaz tou dobou již absolvoval jaderné testy, ale ještě nedisponoval arzenálem, kterým by mohl USA ohrozit (Tannenwald 1999, s. 943). Prezident Truman se stavěl proti použití jaderných zbraní v Koreji. Když v lednu 1953 nastoupil do funkce prezident Eisenhower, jehož klíčovým slibem během kampaně bylo ukončit válku, situace se změnila. Zatímco admirál Radford na prezidentův dotaz odpověděl, že „*bychom museli zaútočit na komunistickou Čínu ze vzduchu, od Šangaje až úplně na sever*“, ministr vnitra Dulles též podporoval použití, ale omezené. Rozdílné názory se také týkaly strategické užitečnosti jaderných zbraní, konkrétně existence vhodných cílů v Koreji a nebezpečí, že použití neukončí válku a sníží tak odstrašovací potenciál jaderných zbraní, jak vyplývá z odtajněných archivů (Keefer a Glennon 1984). Z hlediska norem je nejzajímavější záznam ze schůze Národní rady bezpečnosti (NSC), který shrnuje závěr, že „*president a ministr Dulles se zcela shodli, že je potřeba nějakým způsobem zničit tabu, které se týká používání jaderných zbraní. […] Zatímco ministr Dulles připustil, že v současném stavu světového veřejného mínění nemůžeme použít jadernou bombu, měli bychom se snažit všemi způsoby o odstranění tohoto vnímání*“ (Keefer a Glennon 1984). Ve shrnutí lze tedy říci, že do úvah o použití jaderné zbraně v Koreji byly zahrnuty materiální i normativní elementy. Ačkoliv si USA stále zachovávaly monopol na jaderné zbraně, strategická výhodnost použití v tomto případě byla nejednoznačná. Zároveň si prezident Eisenhower i jeho okolí uvědomovali vznikající jaderné tabu, které považovali za nepraktické a chtěli se jej zbavit. To ukazuje na normu na přelomu emergence a rozšiřování.

Válka ve Vietnamu nabízela množství strategických cílů a nízké riziko jaderné odvety z Ruska nebo Číny (Tannenwald 1999, s. 451). Přesto USA radši utrpěly potupnou porážku vůči mnohem menšímu a nejadernému oponentovi, než aby jaderné zbraně použily. I přes strategickou výhodnost použití se mi však nepodařilo nalézt zdroje, které by ukazovaly vážně

míněné úvahy nad použitím prezidenty Kennedym a Johnsonem[14]. Pouze prezident Nixon spolu s poradcem Henry Kissingerem činili poměrně vágní výhružky, které ale pravděpodobně nebyly vážně míněny. To však záměrně nebylo zřejmé kvůli Nixonově „Madman theory". V jednom případě dal Nixon pokyn ke zvýšení připravenosti k jadernému útoku: „*Proč americká armáda vyhlásila jadernou pohotovost v říjnu 1969? Šlo o důrazný ale tajný vojenský signál vydaný prezidentem Richardem Nixonem. Nixon chtěl přesvědčit lídry Sovětů a Severního Vietnamu, že je ochoten udělat cokoliv, aby ukončil válku ve Vietnamu v souladu s jeho ‚teorií šílence' nátlakové diplomacie*" (Sagan a Suri 2003, s. 150). Mimo Nixonovo strašení však nedochází k vážně míněné a důkladné analýze nákladů a přínosů použití jaderné zbraně, což svědčí o značné síle tabuizující normy. Již v teoretické části jsem zmiňoval, že internalizované normy je nejtěžší pozorovat, právě proto, že se vztahují k chování, které je považováno za natolik nevhodné, že se o něm ani nediskutuje. Z tohoto hlediska lze říci, že již částečně dochází k internalizaci tabu v případech Kennedyho a Johnsona, to však rozporuje případ Nixona, který je hůře čitelný. Ačkoliv nic nenaznačuje, že by Nixon vážně plánoval použití jaderné zbraně, minimálně se snažil vytvářet image někoho, kdo takové chování nepovažuje za nemyslitelné.

Na závěr této části bych chtěl poznamenat, že ačkoliv se předchozích odstavce věnuji primárně otázce použití jaderných zbraní, tato problematika úzce souvisí s kontrolou jaderného zbrojení. To platí v materiálním smyslu, kdy pro státy nedává smysl zvyšovat zásoby zbraní, které nemohou použít. Jejich motivace z hlediska odstrašování tedy stojí na zájmu dosáhnout parity mezi státy, což vyžaduje rovnoměrné – nikoliv nutně velké – zásoby jaderných zbraní. Také z normativního hlediska jsou výdaje na nelegitimní jaderné zbraně těžko obhájitelné před veřejností. To vzhledem k ceně údržby, přechovávání i modernizace arzenálu znamenalo nutnost významného snížení množství jaderných zbraní po konci závodu ve zbrojení a studené války.

[14] Tannenwaldová dochází ke stejnému závěru: „*Prezidenti Kennedy a Johnson věnovali minimum pozornosti vážným úvahám o možnosti použití jaderné zbraně a odmítli činit výhružky jejich použití, i přes některá doporučení, aby tak učinili*" (1999, s. 451).

4 Kyberprostor

4.1 Úvod a terminologie

V první části této práce jsem představil teoretický základ konstruktivistického přístupu k normám a v třetí části jsem představil normativní koncepty nukleárního tabu a nukleární deviace a pokusil se je aplikovat na některé historické případy a načrtnout tak stručně vývoj jaderného tabu jako normy delegitimizující jaderné zbraně, zakazující jejich použití a mající jednoznačné účinky na kontrolu jaderného zbrojení. Poznatky z obou těchto částí se nyní pokusím použít při zkoumání, zda norma nepoužívání nebo kontroly zbrojení existuje v kyberprostoru a v jakém stádiu svého vývoje se nachází. Kyberprostor je nejmladší doménou[15] a také tou nejabstraktnější. Zbrojení a útoky v kyberprostoru mohou nabývat drasticky rozdílných podob, a proto je potřeba nejprve si přesně stanovit, čím se budu zabývat.

V současnosti neexistuje jedna ustálená definice kyberprostoru. Uvedu tedy dvě, které se věnují různým aspektům problematiky. První pochází z poměrně starší strategie pro operace v kyberprostoru amerického Ministerstva obrany (DoD) z roku 2006: „*Doména charakterizovaná používáním elektroniky a elektromagnetického spektra ke skladování, modifikaci a výměně dat prostřednictvím síťových systémů a spojených fyzických infrastruktur*.“ (Department of Defense 2006). Na této definici je zajímavé, že se soustředí na fyzické prvky – elektronická zařízení, přenos dat a infrastrukturu. Poněkud problematické je nedostatečné zohlednění interakce mezi softwarem a hardwarem – data nejsou jen skladována a přenášena mezi zařízeními, ale mohou je též ovládat. Zahrnutí celého elektromagnetického spektra též neprakticky rozšiřuje kyberprostor i například na rušení radarů. O dva roky pozdější definice DoD se soustředí na jiný přístup: „*Globální doména v informačním prostředí sestávající z vzájemně závislých sítí IT technologií, včetně internetu, telekomunikační sítě, počítačových systémů a jejich procesorů a ovladačů*“ (Castelli dle Reveron 2012, s. 5). Tuto definici považuji za vhodnější z několika důvodů. Je v ní obsažena vzájemná závislost a interakce sítí v globálním měřítku, lépe specifikuje konkrétní důležité sítě

[15] Za doménu označilo kyberprostor například v roce 2010 americké Ministerstvo obrany (DoD) ve svém pravidelném Quadrennial Defense Review: „Ačkoliv jde o člověkem vytvořenou doménu, kyberprostor je dnes stejně relevantní doménou pro aktivity DoD jako přirozeně se vyskytující domény země, moře, vzduchu a vesmíru“ (Department of Defense 2010, s. 37)

a věnuje se též počítačovému kódu, který může napadat výpočetní sílu počítačů a připojené ovládací prvky.

Zkoumání kyber hrozeb komplikuje několik faktorů vyplývajících z podoby kyberprostoru. Na rozdíl od hmatatelnějších útoků je velmi komplikované vysledovat původ kyber útoku. O to náročnější je problém přičitatelnosti státním aktérům. Kromě útočníkovy identity však nemusí být možné zjistit ani jaký byl zamýšlený dopad útoku, jaké vedlejší škody útok napáchal a jak se rozšířil (Reveron 2012, s. 10-11). Vstup do kyberprostoru navíc vyžaduje pouze počítač, schopnost jej využívat a internetové připojení; všechny předpoklady jsou široce dostupné. Útoky v kyberprostoru mohou mít výraznou schopnost ekonomicky poškodit, aniž by byly bezprostředně násilné. Může jít například o přenastavení různých řídících systémů pomocí tzv. logických bomb s rozmanitými následky, mezi které by mohlo patřit například chybné řízení vlakové dopravy, odstavení chladících systémů atomových elektráren nebo přerušení komunikace mezi vojenskými složkami (Rid 2013, s. 11). Všechny tyto útoky mohou být násilné ve svém důsledku a určitě by byly považovány za akt agrese.

Při zkoumání kontroly zbrojení je přirozeně důležité rozumět podobě zbraní. Na rozdíl od kinetických zbraní, kam spadají i jaderné zbraně, kterým se věnovala předchozí část, kyber zbraně a útoky mají často hlavně nepřímé následky, náprava do původního stavu je možná v krátkém časovém období, jejich náklady jsou zejména ve výzkumu (a nikoliv výrobě) a jsou založeny na široce rozšířených technologiích. Kyber útoky zároveň vyžadují větší množství informací o cíli a mají hůře předvídatelné důsledky (Reveron, 2012; 38).

Operace v kyberprostoru lze rozdělit do různých kategorií a ne všechny z nich lze označit jako kyber zbraně. Dokument JP 3-13 amerického DoD klasifikuje tři typy operací v počítačových sítích (CNO).

1. Útok na počítačovou síť (CNA) je „*činnost používající počítačové sítě k vyrušení, odepření, poškození, nebo zničení informací uložených v počítačích a počítačových sítích, nebo počítačů a sítí samotných*“ (Department of Defense 2006).
2. Obrana počítačové sítě (CND) má monitorovat a analyzovat neautorizované aktivity a chránit před nimi.

3. Zneužití počítačové sítě (CNE) má umožnit špionážní sběr informací prostřednictvím počítačových sítí[16] (Department of Defense 2006).

Pro účely této práce jsou důležité CNA útoky, které jsou svou podstatou nejblíže konceptu kyber zbraní.

4.2 Historie kyber útoků

Významné CNA útoky jsou poměrně vzácné a jejich historie dobře ilustruje, jak může CNA útok vypadat a jakou škodu může způsobit. Jejich nedávný rozmach (od roku 2007) také může být indikátorem (ne)působení norem v kyberprostoru. Nejnásilnějším a také nejstarším případem je výbuch trans-sibiřského ropovodu v roce 1982. USA tehdy údajně nahrálo škodlivý kód do ovládacího počítače, který poté Sověti koupili od Kanady. Po určité době správného fungování počítač náhle zvýšil tlak v ropovodu, který explodoval. Přestože je tento útok uváděný v mnoha zdrojích, existují pochybnosti o tom, zda se vůbec stal[17] (Rid 2013, s. 4-6). Další útok se odehrál v roce 2007 v Estonsku během protestů rusky mluvící populace kvůli přesunutí památníku neznámého vojína. Šlo o jeden z největších případů Distributed Denial of Service (DDoS). Webové stránky vlády, mnoha firem a dokonce i největší estonské banky byly často nedostupné v časovém rozmezí tří týdnů. Jako reakci založilo NATO v Tallinnu Cooperative Cyber Defense Centre of Excellence. Nikdy se nepodařilo prokázat, kdo za útoky stál (Rid 2013, s. 7). Později v tom samém roce izraelské letectvo bombardovalo staveniště nukleárního reaktoru v Sýrii. Zároveň došlo k sabotáži syrského radaru, pravděpodobně izraelským CNA útokem. Tento přímo nenásilný kyber útok tedy pomohl odstavit protileteckou obranu a umožnit tak kinetický útok. O rok později se něco podobného, avšak ve větším měřítku, stalo během války v Jižní Osetii, kdy zejména DDoS útok byl koordinován s konvenční vojenskou operací. Útočné skripty byly navíc dostupné na internetu, a tak se mohl každý připojit – stačilo si pouze stáhnout soubor war.rar z některého internetového fóra (Rid 2013, s. 8). Virus Stuxnet z roku 2010, údajně sponzorovaný USA a Izraelem, byl schopen vyřadit z provozu íránské jaderné centrifugy. Šlo o technologicky velmi pokročilý útok speciálně cílený na

[16] Tyto pojmy již nejsou zahrnuty v aktualizované verzi dokumentu z roku 2014, nicméně jejich použití považuji za vhodné i proto, že se objevují i v dalších zdrojích včetně odborných prací.

[17] Informace o tomto útoku přinesl představitel americké Národní rady bezpečnosti (NSC) Thomas Reed. Rid zmiňuje tři problémy s věrohodností Reedových tvrzení: všechny sovětské i později ruské zdroje popírají, že se útok stal, není jisté, zda byl při tehdejší 8-bitové technologii vůbec proveditelný, natož pak skrytě, a nakonec ani odtajněné dokumenty CIA ohledně dodávání defektní technologie do SSSR tento incident nezmiňují (Rid 2013).

konkrétní ovládací systém, jehož důkladná znalost byla nutným předpokladem. Je pravděpodobné, že pokud by Stuxnet nebyl včas odhalen, bylo by možné jej využít k dálkovému ovládání systémů s potenciálem způsobit katastrofické selhání (Reveron 2012, s. 5). Mezi další nedávné CNA útoky patří Shamoon virus, který napadl zejména státem vlastněnou společnost Saudi-Aramco a vedl k rozsáhlému zničení dat a vyrušení produkce ropy a útok Operace Ababil, který napadl americké finanční instituce útokem DDoS. Podezřívaným sponzorem obou útoků je Írán (Mazanec 2014, s. 51).

Tabulka č. 1 shrnuje zmíněné a některé další CNA útoky.

Tabulka č. 1: Shrnutí CNA útoků v kyberprostoru

NÁZEV ÚTOKU	ROK	CÍL	TYP	POZNÁMKY
TRANS SIBIŘSKÝ ROPOVOD	1982	Civilní	Logická bomba vedoucí k výbuchu	Zpochybňováno, zda se vůbec stal
ESTONSKO	2007	Civilní	DDoS	
RADAR V SÝRII	2007	Vojenský	Sabotáž radaru	Ve spojení s kinetickým útokem
JIŽNÍ OSETIE	2008	Civilní	DDoS	Účast civilistů na útoku
CONFICKER	2008	Civilní	DDoS	
STUXNET	2009-2010	Vojenský	Sabotáž jaderných centrifug	Zřejmě nejpokročilejší a nejdražší
SAUDI-ARAMCO	2012	Civilní	Zničení dat s cílem zastavit produkci ropy	
OPERACE ABABIL	2012-2013	Civilní	DDoS	
TV5 MONDE	2015	Civilní	Sabotáž dat vedoucí k zastavení vysílání	

Zdroj: Mazanec (2014), Rid (2013), Correra (2016)

Z výše nastíněných kyber útoků vyplývá několik poznatků. Ke kyber útokům zjevně dochází a jsou mířeny jak na vojenské, tak i civilní cíle. Mazanec (2014) vidí vznikající tendenci v tom, že útoky, na kterých se měly podílet západní státy, jsou cíleny na vojenské cíle a považuje to za

možnou vznikající kompetitivní normu. Vzhledem k velmi nízkému množství relevantních útoků i problematické přičitatelnosti jsem názoru, že analýza současné praxe států není postačující k učinění takového závěru. Dále lze pozorovat, že jde často o poměrně jednoduché útoky typu DDoS, které nezpůsobují rozsáhlé materiální škody ani trvalé poškození hardwaru. Ostatní útoky ale způsobily větší ekonomické škody, obvykle s cílem zabránit aktivitě, pro kterou byly zasažené počítače používány a poškodit potřebná data. Též tyto útoky mířily na vojenské i civilní cíle. Žádný kyber útok zatím přímo nezpůsobil úmrtí (teoreticky jim dokonce mohl předejít, například kdyby se Izrael rozhodl použít jiný způsob odstavení syrského radaru). Na základě tohoto shrnutí lze konstatovat, že z nedávné praxe nevyplývá, že by se aktéři cítili být omezeni určitou normou ve svém útočném chování v kyberprostoru. Důležité tedy bude zkoumat, zda dochází alespoň k emergenci určitých norem.

4.3 Normy v kyberprostoru

V roce 2013 uvedl americký ředitel národního zpravodajství James Clapper v pravidelném zhodnocení celosvětových rizik americké zpravodajské komunity: „*Rostoucí využívání kyber schopností k dosahování strategických cílů postupuje rychleji než vývoj sdíleného chápání norem chování, což zvyšuje šanci špatného odhadu a neporozumění, které mohou vést k nezáměrné eskalaci*“ (Clapper 2013, s. 1). Vývoj norem je potřeba chápat jak z hlediska současné praxe, tak z probíhajícího strategického, diplomatického a akademického diskurzu a s ním spojeného vývoje v chápání tohoto problému.

S nejednoznačnými výsledky zkoumání nedávné praxe, kterým přispívá problém přičitatelnosti a nedostatečné množství případů, je tedy potřeba zaměřit se na vývoj ve vnímání kyber zbraní. Toho lze docílit analýzou odborné literatury a debaty v diplomatickém, strategickém a právním prostředí. Předem je však potřeba specifikovat určitá kritéria toho, na co je se zaměřit. Mazanec (2015) prezentuje několik hypotéz, jak by mohla vypadat emergence normy u zbraní založených na emergentních technologiích[18] (vychází ze zkoumání emergence chemických a jaderných zbraní a strategického bombardování). Tyto hypotézy nastiňují určité faktory, které mohou ovlivnit úspěch emergence normy a odpovídají vývoji pozorovanému v případě jaderného tabu. Pro ranný vývoj normy může být velkou výhodou její spodobnění s jinou, již

[18] Zbraně emergentních technologií je poněkud širší kategorie než kyber; spadají sem též autonomní zbraňové systémy nebo vysoce výkonné lasery. Smyslem takto široce definované kategorie je možnost zkoumat různé technologie v různých časových obdobích – na konci a bezprostředně po 2. s. v. by sem spadaly i jaderné zbraně.

zavedenou normou (například označení za nekonvenční). Emergence normy též bývá úspěšnější, pokud k ní začne docházet dřív – optimálně před širokým rozšířením zbraně (jako tomu bylo například při rozhodování USA ohledně použití jaderné zbraně v Koreji). Velkou překážkou pro vznik normy jsou rozdílné představy ohledně dopadu stále se technologicky vyvíjející zbraně, což odpovídá tvrzením Jamese Clappera ohledně kyberprostoru. Může však dojít i k případům, že nadnesené vnímání nebezpečí, které nová technologie přináší, zvýší tlak na emergenci normy – k tomu bych však doplnil, že v takových situacích, kdy ještě nevzniklo porozumění fungování a praktického dopadu zbraně, nemusí být zřejmá jedna norma, na kterou se norm entrepreneurs mají zaměřit. Dalším důležitým faktorem je efektivita možné obrany před útokem novou zbraní. Absence efektivních obranných opatření podporuje zájem o normu omezující využívání zbraně, ale též její proliferaci. Hlavní proměnnou v emergenci norem je zájem států. Ačkoliv nové rámování problému ze strany norm entrepreneurs může vnímání zájmů měnit, vhodná materiální situace hraje též významnou roli. Například monopol jednoho nebo malé menšiny států na určitou zbraň nebo vysoké vstupní překážky technologií mohou přesvědčit většinu států k adopci normy (Mazanec 2015). V následující tabulce se pokusím předběžně shrnout splnění podmínek těchto hypotéz v případech jaderných zbraní a kyberprostoru.

Tabulka č. 2: Hypotézy faktorů úspěšnosti norem v emergentních technologiích

HYPOTÉZA	**JADERNÉ ZBRANĚ**	**KYBERPROSTOR**
spojení s jinou normou -> počáteční výhoda	Částečně, zmiňována podobnost se strategickým bombardováním	Záleží na konkrétní kandidátní normě
emergence před rozšířením -> úspěšnější emergence	Ano, uznána Američany, když měli stále ještě monopol	Ne, k rozšíření již došlo
Rozdílné představy -> překážka pro vznik normy	Ne, dopad jaderných zbraní byl po roce 1945 poměrně zřejmý	Ano, viz Clapper
Neefektivní obrana -> silnější proliferace a norma proti použití	Ano, místo obrany odstrašování	Ano
Monopol nebo tech. překážky -> lepší emergence	Ano, USA měla monopol	Ne, velmi nízké bariéry pro vstup

Výše zmíněné hypotézy budu nadále zkoumat na konkrétních případech norem v kyberprostoru, protože mohou pomoci posoudit pravděpodobnost úspěšné emergence

konkrétní normy. Budu se věnovat kontrole zbrojení, (ne)používání a normativnímu odstrašování a v každé z těchto oblastí se pokusím nalézt normu, jejíž emergence je nejpravděpodobnější a tuto pravděpodobnost posoudit. Nebudu se tedy tolik zabývat vysoce ambiciózními normami, jako úplný zákaz kyber zbraní nebo jejich používání, ale spíše realističtějšími omezenými formami těchto norem. V případě kontroly zbrojení to je bránění nestátním aktérům v kyber útocích, v případě (ne)používání kyber zbraní jde o zákaz CNA útoků na kritickou národní infrastrukturu a v případě normativního odstrašování o nutnost přičitatelnosti pro protiútok.

4.3.1 Kontrola zbrojení: bránění nestátním aktérům v kyber útocích

V současnosti neexistuje žádná mezinárodní dohoda ohledně kontroly zbrojení v kyberprostoru – a zatímco absence formálního instrumentu neznamená sama o sobě absenci normy, taková norma by čelila stejným problémům, které komplikují debatu o podobě a přijetí příslušné smlouvy: „*Tradiční režimy kontroly zbrojení jsou nepoužitelné v kyberprostoru ze čtyř důvodů: je obtížné měřit relativní sílu států v kyberprostoru; existuje nejistota ohledně vojenských dopadů kyber technologií; je obtížné monitorovat dodržování; a je problematické vynucování*“ (CFR 2018). Tyto problémy nejsou specifické pro kyberprostor, ale jeho podmínky je činí závažnějšími – zatímco dopad kinetického útoku lze alespoň částečně určit dle počtu a typu zbraní, kyber zbraně lze hodnotit pouze kvalitativně, a dokonce ani útočník nemusí přesně vědět, na kolik se útok rozšíří a jak na něj budou reagovat napadené systémy. Kvůli široké dostupnosti technologií potřebných ke kyber útoku, možnosti outsourcingu na nestátní aktéry a problému přičitatelnosti je technicky, natož pak politicky, jakákoliv vícestranná norma o omezení státních kapacit provádět kyber útoky bezzubá. Alternativou, která spadá do kontroly zbrojení a není tak závažně ovlivněna uvedenými problémy, může být kriminalizace kyber útoků provedených nestátními aktéry v rámci vnitrostátního práva. Závazek kriminalizovat neoprávněný přístup k počítačovým systémům a změnu nebo ničení dat v nich obsahuje budapešťská Úmluva o kyberprostoru Rady Evropy (Council of Europe Treaty Office 2018). Jejím signatářem se v roce 2006 staly i Spojené státy. USA lze vnímat v tomto případě jako norm entrepreneur, což ukazuje Cyberspace Policy Review z roku 2009: „*Mezinárodní normy jsou klíčové pro zajištění bezpečné a prosperující digitální infrastruktury. Národ potřebuje strategii pro kyber bezpečnost navrženou ke směřování mezinárodního prostředí a spojení podobně smýšlejících států v řadě otázek, včetně přijatelných norem ohledně technických standardů, teritoriální jurisdikce, odpovědnosti suverénních států a použití síly*“

(Department of Homeland Security 2009, s. 20). Přístup kriminalizace útoků nestátních aktérů a spolupráce mezi státy na dobrovolné bázi odpovídá americké praxi neutrálního a minimálně regulovaného internetu (viz Hillary Clinton 2010). Některé ostatní státy, které působí jako vlivní norm entrepreneurs však mají odlišné cíle: „*Naproti tomu Rusko má tendenci vnímat kyber bezpečnost jako záležitost vnitřní bezpečnosti spíš než zahraničních vztahů. Ruské snahy o uzavření multilaterálních úmluv se zakládaly na potřebě ovládat informace na svém území, spíš než podpořit neomezený tok informací napříč hranicemi*“ (Stevens 2012, s. 20). V ruském pojetí není výrazně rozlišeno mezi CNA útoky a informační válkou založenou na rozšiřování informací cílících na destabilizaci států. Zatímco USA se odkazuje na „podobně smýšlející státy“, ruský přístup se opírá o podporu konkrétně Číny, Tádžikistánu a Uzbekistánu, se kterými společně Rusko zformulovalo svoje návrhy v dopise generálnímu tajemníkovi OSN psaném formou rezoluce. Tento dokument prezentuje kodex chování, který mají státy slíbit dodržovat. Jsou v něm zajímavě zkombinovány požadavky spolupráce v boji proti kriminálním a teroristickým aktivitám, ochrany lidských práv a zákaz šíření informací ohrožujících „*politickou, ekonomickou a sociální stabilitu, stejně jako jejich duchovní a kulturní prostředí.*“ (OSN 2011). Tyto požadavky jsou však protichůdné, pokud přijmeme výklad, že svobody projevu, náboženství nebo shromažďování chráněné lidskými právy jsou aplikovatelné i v kyberprostoru[19]. Důležitějším požadavkem je zde ochrana stability a kulturního prostředí: „*Rusko tlačí na kontrolu zbrojení v kyberprostoru, kontrolu zbrojení informačními zbraněmi. Většina lidí to považuje za neupřímné a já mám tendenci souhlasit. Většina pozorovatelů to vnímá jako snahu Ruska omezit navládu USA v kyber doméně. Rusko se více zajímá o barevné revoluce a mobilizaci disidentských a lidskoprávních skupin na internetu*“ (Deibert 2015, s. 6). Ať už tedy nesoulad lidskoprávního požadavku považujeme za založený na jiném výkladu, nebo zcela neupřímný, ukazuje se značný rozpor ve vnímání kyber hrozeb, na které by se případná norma měla vztahovat. Domnívám se tedy, že z výše zmíněných hypotéz je v tomto případě velmi důležitá rozdílnost představ států v otázce toho, co lze kvalifikovat jako kyber útok. Protichůdné jsou nejen zájmy (ochrana stability vs. šíření demokracie a lidských práv), ale i v případě, že by tento problém byl překonán, by institucionalizace, která může pomoci procesu kaskády, stála před překážkou rozdílných představ ohledně podoby právní úpravy

[19] Tento výklad, spojený s představou, že svoboda projevu pomůže šířit demokracii a lidská práva, je podporován USA, zejména ministryní zahraničních věcí Obamovy administrativy, Hillary Clinton (Hillary Clinton 2010).

(závazné úmluvy vs. kriminalizace a dobrovolná mezinárodní spolupráce) a absence možnosti verifikovat dodržování spojené s problémem přičitatelnosti a možnosti států spoléhat na třetí strany. V současnosti nedochází ani k důsledné stigmatizaci států, které umožnily útoky nestátních aktérů v rámci své teritoriální nebo personální jurisdikce, což by mohlo analogicky ke konceptu nukleární deviace vést k posunu hranice mezi normálním a deviantním chováním - současný americký prezident Donald Trump velmi kategoricky spojuje přímé a prokazatelné spáchání státem s jeho zodpovědností (Trump in Fox News 2016).

4.3.2 Zákaz použití: zákaz útoků na kritickou národní infrastrukturu (CNI)

Již dříve v této práci jsem se věnoval důležitosti zájmu klíčových států na emergenci normy. Z tohoto hlediska v zajímavé situaci se nachází USA. Slovy poradce prezidenta Obamy Richarda Clarkea: „*Zatímco Spojené státy mají velmi pravděpodobně nejsofistikovanější schopnosti kyber ofenzívy, tato ofenzivní zdatnost nemůže nahradit slabiny v našich obranných pozicích*“ (2010, s. 145). Vzhledem k podstatě kyberprostoru je vztah mezi útokem a obranou velmi asymetrický. Zatímco v případě útoku lze mluvit o libovolném množství cílů, budování obrany je realisticky možné pouze pro omezené množství zvlášť důležitých systémů[20]. Tyto systémy, označované zkratkou CNI, jsou britskou vládou definovány jako: „*ty kritické prvky národní infrastruktury (podniky, systémy, místa, majetek, informace, lidé, sítě a procesy), jejichž ztráta nebo zkompromitování by vyústilo v značný negativní dopad na dostupnost, přístup, nebo integritu základních služeb, což by vedlo k závažným ekonomickým nebo sociálním důsledkům, nebo ke ztrátě životů*“ (Center for Protection of National Infrastructure). Ochrana těchto systémů je důležitým zájmem USA, Velké Británie, ale i ostatních kyber velmocí, protože zpravidla čím více stát spoléhá na počítačové sítě a infrastrukturu, tím náchylnější je ke kyber útokům. Disproporce mezi útočnými, obranými schopnostmi a závislostí na počítačových sítích může mít vážné následky na uvažování států o používání svých útočných možností: „*Pokud nesnížíme zranitelnost kyber útoky, budeme trpět sebe-odstrašováním*“ (Clarke 2010, s. 156). Tato myšlenka efektivně rámuje neútočení jako národní zájem a je tedy dobrým předpokladem pro emergenci normy. Touto normou by mohl být závazek neútočit první (no first use – NFU), který by měl tu výhodu, že by navazoval na stejný koncept v případě jaderného zbrojení[21]. Taková norma by však čelila několika problémům. V závislosti na šíři její

[20] USA například používá systém Einstein pro ochranu vojenské domény .mil a vládní .gov (Clarke 2010)
[21] NATO tento závazek nikdy oficiálně u jaderných zbraní neuznalo, vzhledem k závěrům třetí části však lze konstatovat, že to spíš svědčí o absenci institucionalizace než o neexistenci normy.

definice – zda by byly zahrnuty i špionážní aktivity – by její porušení mohlo být neodhalitelné, což by významně oslabilo normativní odstrašování. Přičitatelnost je dalším problémem, zvlášť v případě, že by se zákaz vztahoval na všechny potenciální cíle (státní i nestátní). Nejrealističtější formou případné normy by tedy mohl být zákaz prvního útoku omezený na CNA útoky na CNI[22]. Prominentní platformou, kde je toto téma diskutováno, je Globální konference o kyberprostoru (série konferencí tzv. Londýnského procesu, jehož cílem je podpořit globální normy zodpovědného chování v kyberprostoru). Ačkoliv tyto konference postrádají ambice činit rozhodnutí zavazující státy, podařilo se zde dosáhnout shody na jednom principu, který byl zakotven ve výsledném dokumentu Soulské konference podepsaném 87 státy: „*Mezinárodní právo, a konkrétně Charta OSN, je aplikovatelné a klíčové pro zajištění bezpečnosti a stability a podpoření otevřeného, bezpečného, mírového a dostupného kyberprostoru*“ (Data Security Council of India 2013). Ačkoliv není jasné, jak budou pojmy mezinárodního práva, které jsou jasně definované pro jiné domény, ale nejasné v kyberprostoru, interpretovány, považuji to za krok směrem k zákazu prvního útoku na CNI. Článek 2 odst. 4 Charty OSN (United Nations 1945) zakazuje výhružku nebo použití síly proti suverénním státům. Vzhledem k nejednoznačnosti toho, co lze v kyberprostoru kvalifikovat jako útok proti suverénnímu státu, nebo ozbrojený útok obecně, jde při restriktivní interpretaci o pojem velmi blízký zákazu prvního[23] CNA útoku na CNI. Rozhodně však nelze hovořit o normě srovnatelné s jaderným tabu, vzhledem k tomu, že zákaz použití síly je zcela běžně porušován. Navíc následující konference v Haagu a Novém Dillí nepřinesly žádný konkrétnější požadavek nebo definici v tomto ohledu.

Vzhledem k výše uvedeným hypotézám má tato norma šanci uspět díky spojení s jinou normou (zákaz prvního použití a zákaz použití síly), díky méně rozdílným představám států než například u bránění nestátním aktérům v kyber útocích, díky neefektivitě obrany a díky vyšším vstupním bariérám než u útoků na jiné cíle. Přesto však v nedávných letech nedochází k pokroku v emergenci a budoucnost normy tedy závisí na tom, zda začne některý z klíčových států působit jako norm entrepreneur. Z hlediska motivace by to dávalo největší smysl u států s vyšší závislostí na počítačových sítích a horší schopností jejich obrany – zejména tedy USA a některých dalších členů NATO.

[22] V případě CNI problém přičitatelnosti sice stále figuruje, ale vzhledem k vyšším nákladům útoku a nižším motivacím než např. při útoku na komerční civilní cíle není tak výrazný.
[23] Prvního proto, že dle článku 51 se zákaz použití síly nevztahuje na sebeobranu (United Nations 1945).

4.3.3 Normativní odstrašování a požadavek přičitatelnosti v sebeobraně

Normativní odstrašování je koncept, který spojuje normativní standard vhodného chování s racionální maximalizací užitku při odstrašování. Normy mohou měnit, jak státy vnímají vlastní zájem. Jejich působení též přináší další klady a zápory, které musí při odstrašování státy zvážit, například riziko delegitimizace při porušení normy. Tomuto vztahu mezi normami a odstrašováním jsem se věnoval již v třetí části této práce. Odstrašování samotné lze dělit na dvě formy – 1) odepřením (by denial), kdy je eliminován užitek, který útočníkovi plyne z útoku, a 2) odstrašování trestem (by punishment), které zvyšuje náklady na útok. Odstrašování v kyberprostoru je vzhledem k podobě útoků, například v případě použití zatím neznámých slabin systému, pouze částečně úspěšné. Odstrašování v kyberprostoru navíc obvykle probíhá odepřením, což je na hraně toho, co lze za odstrašování považovat. Útok, ke kterému došlo, ale byl odepřen, zjevně nebyl odstrašen. V tomto případě je tedy zvlášť důležité mluvit o normativním odstrašování, protože negativní důsledky plynoucí z porušení normy mohou být zároveň trestem.

Důležitým specifikem odstrašování v kyberprostoru je velká proliferace útočných schopností. Na rozdíl od jaderných zbraní, kterými disponuje pouze několik států, kyber zbraně má k dispozici široké spektrum státních i nestátních aktérů. Proto vyžaduje kyberprostor rozmanitější odstrašovací strategie: „*Kvůli rozdílnosti a množství státních a nestátních aktérů v kyberprostoru a kvůli relativní dostupnosti destruktivních kyber nástrojů efektivní odstrašovací strategie vyžaduje řadu opatření a schopností k ovlivnění chování těchto aktérů*“ (Department of Defense 2015, s. 10). Z tohoto hlediska lze rozlišit dva typy odstrašovacích strategií: obecné, které mají zamezit útoku nezávisle na jeho typu a zdroji, například firewall, a specifické, které jsou efektivnější, ale pouze vůči konkrétním útokům, například antivirová ochrana spoléhající na databázi známých virů.

Jednou ze strategií obecného odstrašování trestem, která závisí na normách, může být protiútok. Ten vychází z výše zmíněné aplikovatelnosti mezinárodního práva na kyberprostor. Porušení normy proti agresi mezi státy vede k legitimní sebeobraně. Ta je limitována požadavkem proporcionality, ale není určen způsob, a dokonce ani doména, ve které má být sebeobrana provedena. To otevírá možnost kinetickým sebeobranným opatřením v reakci na kyber útoky (Jensen 2012 s. 792-795). Ačkoliv k takovému případu zatím nedošlo, strategie pro kyberprostor Obamovy administrativy ukazuje, že tuto možnost USA zvažuje:

„*Vyhrazujeme si právo použít všechny nutné prostředky – diplomatické, informační, vojenské a ekonomické – jak bude potřeba a v souladu s aplikovatelným mezinárodním právem, pro ochranu našeho národa, našich spojenců, partnerů a zájmů*“ (Obama White House 2011, s. 14). Tato forma odstrašování však v současnosti trpí několika problémy, které jsou pro kyberprostor typické. Lze ji použít pouze v případech nesporné přičitatelnosti původního útoku a také není zatím jasné, jak aplikovat definice konceptů jako je ozbrojený útok nebo proporcionalita na dění v kyberprostoru nebo při porovnávání kyber útoků s kinetickými. Částečným technologickým řešením těchto problémů může být aktivní kyber obrana (ACD). Jde o různé nástroje na pomezí obrany a útoku, které pracují na principu interakce s probíhajícím útokem. Například „honeypots“ mohou být uměle vytvořené cíle, které napodobují pro útočníka zajímavá data, ale ve skutečnosti sbírají informace o útočníkovi. To lze kombinovat s metodou „hack-back“, která spočívá v obraně proti probíhajícímu útoku pomocí protiútoku (Dewar 2017)[24].

Problém přičitatelnosti v odstrašování však není jen technickou otázkou. Přičitatelnost je, ve své podstatě, schopnost přiřadit fyzickou identitu aktérovi, jehož identita v kyberprostoru může a nemusí být známa (příklad: znám počítač nebo I.P. adresu, ze kterého útok pochází a snažím se tuto informaci spojit s konkrétní fyzickou osobou, organizací, nebo státem). Z toho vyplývá, že na sebeobranu v kyberprostoru nemusí být přičitatelnost nutně splněna. Stejně tak tomu může být i mimo kyberprostor, například v situacích podobných válce v Jižní Osetii; ačkoliv nelze přesně specifikovat, kdo stál za kyber útoky na Gruzii, vzhledem k probíhajícímu konfliktu lze považovat Rusko za velmi pravděpodobného pachatele. Přičitatelnost se zde ukazuje nikoliv jako binární záležitost, ale otázka specificity a pravděpodobnosti určitého útočníka. Lupovic vzhledem k uvedenému navrhuje vnímat požadavek přičitatelnosti za normu: „*Pokud je aktér neochotný přijmout soudobou normu, která neospravedlňuje protiútok založený na nepřímých důkazech identity útočníka, může jí vzdorovat protiútočením a měnit tak normu skrze praxi*“ (2016). Tato norma pracuje odlišně od těch dříve uvedených – místo zákazu určité chování naopak přikazuje – ale přesto se zdá poměrně efektivnější. Přičitatelnost je někdy dokonce považována za tak důležitou, že její absence znamená absolutní nejistotu v tom, kdo útok spáchal. Slovy amerického prezidenta Donalda Trumpa: „*Hackování je velmi*

[24] Strategií související s protiútokem je použití protiopatření, které nespadá do mezinárodního, ale vnitrostátního práva. Kriminalizace a trestání nestátních aktérů za jimi provedené kyber útoky již však bylo rozebráno v části týkající se kontroly zbrojení, proto se jím zde již nebudu dále zabývat.

zajímavé. Jak jednou hacknou, pokud jste je nechytili při činu, už je nechytíte. Neví se, jestli jsou Rusko, Čína, nebo někdo jiný. Mohl by to být někdo, kdo někde leží v posteli“ (Trump in Fox News 2016). Tento pohled je však třeba považovat za extrémní; termín přičitatelnost znamená pravděpodobnost správnosti určení identity útočníka tak vysokou, že ji lze dle příslušných právních standardů považovat za prokázanou[25]. I nižší úroveň pravděpodobnosti však může být užitečná. Autoři, kteří se zabývají proběhlými kyber útoky, často uvádějí pravděpodobné útočníky a podobně postupují i státní orgány: „*Hodnocení přičitatelnosti obvykle není jednoduchým tvrzením ohledně toho, kdo provedl operaci, ale spíše řada posudků ohledně toho, zda šlo o izolovaný incident, kdo byl pravděpodobný pachatel*“ (Office of the Director of National Intelligence 2017, s. 2). Toto vnímání se věnuje nákladům a přínosům porušení normy (které jsou ovlivněny pravděpodobností správného určení pachatele), což je dle konceptu nukleárního tabu jedním z typů důkazu existence normy a odpovídá normě, která prošla kaskádou, ale nikoliv internalizací; norma omezuje chování státu tím, že mění vnímání jeho výhodnosti, ale její porušování není nepředstavitelné. Lze tedy hovořit o poměrně úspěšné normě, nicméně je důležité vnímat i riziko jejího rozpadu – při situacích jako byla válka v Jižní Osetii, může být z kontextu vysoce pravděpodobné, kdo je útočník, aniž by byla splněna přičitatelnost. A zároveň, jak naznačuje Lupovic, v takovýchto případech eskalace, kdy porušení normy může přinést státu výrazný prospěch, může dojít k rozpadu normy (jako v případě strategického bombardování za druhé světové války). Dle konceptu nukleární deviace by taková situace mohla vést k postupné změně ve vyžadované pravděpodobnosti, která je ještě přijatelná.

4.4 Výsledky

Kyberprostor je v mnoha ohledech jedinečnou doménou a jeho specifika přinášejí výzvy, se kterými se ostatní domény nemusely potýkat. V některých případech jde o známé problémy, které jsou v kyberprostoru intenzivnější – například přičitatelnost, jindy jde o zcela nové fenomény, jako je nepředvídatelnost šíření útoku mezi systémy a jeho dopad na ně. Dosavadní praxe útoků v kyberprostoru navíc nabízí pouze malé množství příkladů, z něhož nevyplývají jasné tendence chování států v kyberprostoru. Vhodnost zvoleného analytického přístupu je do velké míry závislá na tom, jak se tento přístup dokáže vypořádat s výzvami prezentovanými

[25] Viz například Draft Articles on Responsibility of States for Internationally Wrongful Acts, návrh mezinárodní smlouvy, která by měla vytyčit konkrétní podmínky přičitatelnosti.

samotnou podstatou kyberprostoru. Jak ukazují prezentované hypotézy založené na dřívějších emergentních technologiích, normy v kyberprostoru mají několik výhod, ale i úskalí. Problematické je pro normy již proběhlé rozšíření kyber zbraní, které předcházelo emergenci norem, rozdílné představy aktérů a nízké bariéry pro vstup. Neefektivita obrany v kyberprostoru na druhou stranu zvyšuje poptávku po regulaci chování států, kterou mohou normy nabídnout. A spojení chování v kyberprostoru s širokou paletou norem z již existujících domén může podpořit jejich emergenci. Tyto výhody jsou zjevné ve zkoumaných oblastech. Zatímco kontrola zbrojení v kyberprostoru čelí množství praktických problémů, dílčího úspěchu je možné dosáhnout normou kriminalizace kyber útoků nestátními aktéry. Normy též nabízí vysvětlení, jak může aplikace mezinárodního práva na kyberprostor vést k (ne)používání kyber zbraní v útocích na kritickou infrastrukturu. Chápání požadavku přičitatelnosti v sebeobraně a normativním odstrašováním jako normy umožňuje sledovat plynulý vývoj v požadavku přičitatelnosti jako měnící se minimální přijatelné pravděpodobnosti správného určení pachatele.

To, že normativní přístupy mohou obohatit analýzu kyberprostoru však samo o sobě neznamená, že lze v kyberprostoru použít koncepty rozpracované pro jaderné zbraně. To souvisí s rozdílností těchto dvou domén. Nukleární tabu užitečně specifikuje, jak uvažování státu o chování regulovaném normou dokazuje stádium vývoje této normy. Samotné nukleární tabu ale počítá s omezeným a známým počtem klíčových aktérů, což jsou v jeho případě státy držící zbraně. To však významně neodpovídá kyberprostoru, kde kyber zbraněmi disponují státní i nestátní aktéři a šíření těchto zbraní může probíhat prakticky okamžitě. Držení kyber zbraně je navíc vágním pojmem a samotné moc neimplikuje; kyber útoky mohou spoléhat na neodhalené slabiny systému, jsou často na jedno použití a rozšíření jejich zdrojového kódu je může neutralizovat. Problém přičitatelnosti neumožňuje důsledně stigmatizovat každé použití, což výrazně ztěžuje vznik tabu.

Nukleární deviace poskytuje flexibilitu svou schopností vnímat plynule vývoj normy a zohledňovat přijatelnost určitého chování v závislosti na jeho míře. Toho lze využít například při analýze přičitatelnosti v sebeobraně. Zároveň však tento přístup vyžaduje možnost kvantifikovat míru určitého chování, což kyberprostor často neumožňuje. Počet držených kyber zbraní je zcela neužitečným indikátorem – je to kvalita, nikoliv kvantita kyber zbraní, která určuje jejich dopad. Tento dopad navíc nemusí být předvídatelný samotným útočníkem

a vzhledem k decentralizované podobě kyberprostoru ani následně měřitelný. Tento přístup navíc stojí na interakci stigmatizujících a stigmatizovaných a jejich soutěži o normu – nepočítá s alternativou, že pachatel není vždy známý a nelze ho stigmatizovat – a nedokáže tedy vysvětlit, jak soutěž o normu probíhá za takové situace a jak ji ovlivní nepřičitatelné porušení.

V závěru tedy považuji normy za užitečný nástroj při zkoumání kyberprostoru, ale jejich aplikaci na jaderné zbraně za převážně nevhodnou pro specifické podmínky kyberprostoru. Zatímco individuální elementy použitých přístupů pomohly rozšířit teoretický rámec evoluce norem o poznatky použitelné v kyberprostoru, jako celky se ukázaly moc přizpůsobené specifickým podmínkám jaderných zbraní, než aby byly v současné formě přenositelné i do kyberprostoru. Tyto silné i slabé stránky mohou do budoucna poučit vznik nových konceptů norem lépe přizpůsobených kyberprostoru, což bych považoval za významný přínos jeho analýze.

Závěr

Tato práce se zabývá teorií evoluce norem, její aplikací na jaderné zbraně a využitím poznatků z jaderné technologické domény v kyberprostoru. Cílem bylo zodpovědět výzkumnou otázku, zda normativní přístupy k jaderným zbraním mohou fungovat jako efektivní analytické nástroje při zkoumání kyberprostoru. Práci jsem rozdělil na čtyři části.

V první části jsem se zabýval teoretickým rámcem evoluce norem. Pokusil jsem se definovat normy a představit mechanismy, kterými jsou normy ovlivňovány a kterými ovlivňují chování států. Zaměřil jsem se na životní cyklus norem, který mi umožnil zkoumat vývoj normy od emergence až po internalizaci a diferenciovat mezi normami v závislosti na jejich stádiu v životním cyklu.

V druhé části jsem se věnoval metodologii práce, za kterou jsem zvolil případovou studii. Subjektem této studie je test aplikovatelnosti normativních konceptů z jaderné na kyber doménu. Jejím předmětem je dosavadní praxe útoků v kyberprostoru, strategické dokumenty USA a vyjednávání států na mezinárodních platformách OSN a konferencí tzv. Londýnského procesu.

Třetí část jsem zahájil terminologickým exkurzem do kontroly zbrojení a odzbrojování a navázal jsem historickým shrnutím vývoje kontroly jaderných zbraní. Následně jsem uvedl dva normativní přístupy, jejich přínos a vztah vůči realistickému přístupu odstrašování. Za tyto

přístupy jsem zvolil nukleární tabu a nukleární deviaci. Rozhodl jsem se tak kvůli jejich rozdílným přednostem – nukleární tabu dokáže z podoby úvah států nad chováním regulovaném normou určit, v jakém stádiu vývoje se norma nachází. Nukleární deviace oproti tomu přistupuje k normám jako plynulému vývoji a soutěži mezi stigmatizujícím a stigmatizovaným o posunutí hranice přijatelného chování. Každý z těchto přístupů pracuje s životním cyklem normy odlišně, přesto oba fungují v rámci evoluce norem a doplňují jej o nové perspektivy, které pomáhají tento přístup specifikovat pro jaderné zbraně. Tyto přístupy jsem poté demonstroval na historickém vývoji (ne)používání jaderných zbraní.

Ve čtvrté a nejdůležitější částí práce jsem se věnoval terminologii kyberprostoru a specifickým podmínkám jeho fungování, které kyberprostor odlišují od ostatních domén. Poté jsem shrnul dosavadní praxi CNA útoků, kterou jsem pro omezený počet případů a problému s přičitatelností konstatoval za nedostatečnou pro prokázání vlivu norem na tuto praxi. Dále jsem se proto věnoval normám ve třech oblastech: kontrole zbrojení, (ne)používání a normativním odstrašování. Tato analýza mě vedla ke dvěma kandidátním a jedné rozšířené normě. Za kandidátní normy považuji kriminalizaci kyber útoků nestátními aktéry a zákaz prvního CNA útoku na kritickou národní infrastrukturu. Emergence těchto norem vyžaduje aktivní působení některého státu jako norm entrepreneur. V prvním případě považuji USA a Rusko za norm entrepreneurs, nicméně každý z těchto států usiluje o jinou podobu této normy. V druhém případě považuji v kyberprostoru silné a skrz propojenost své infrastruktury zranitelné státy za dobré kandidáty na norm entrepreneurs, ale zároveň jsem došel k závěru, že USA, které nejlépe splňují tyto kritéria, v současnosti jako norm entrepreneur nepůsobí. V analýze normativního odstrašování v kyberprostoru jsem se věnoval aplikaci mezinárodního práva na kyberprostor a legitimní sebeobraně, což mě přivedlo na otázku přičitatelnosti a její nutnosti pro sebeobranu. K požadavku přičitatelnosti jsem se rozhodl přistupovat jako k normě, kterou považuji za rozšířenou, byť ohroženou možnou výhodností jejího porušení v případě eskalace zejména kombinovaného kyber a kinetického konfliktu. V hodnocení výsledků této části jsem došel k závěru, že teoretický rámec evoluce norem je vhodným analytickým nástrojem pro zkoumání kyberprostoru, ale že jeho aplikace na jaderné zbraně nejsou přenositelné do velmi rozdílné domény kyberprostoru. Z tohoto důvodu bych považoval za přínosnou teorii, která se pokusí sblížit evoluci norem s podmínkami kyberprostoru.

Za hlavní přínos této práce považuji demonstraci užitečnosti evoluce norem při zkoumání kyberprostoru. Ačkoliv se aplikace této teorie, které byly úspěšné v kontextu jaderných zbraní, nehodí do kyberprostoru kvůli novým výzvám, které analýza této domény přináší, jejich dílčí úspěchy a selhání v aplikaci na kyberprostor mohou sloužit jako inspirace pro budoucí snahy vytvořit teorii norem, která bude specifická pro kyberprostor.

Zdroje:

Články, akademické a odborné práce

1) ADLER, Emanuel. The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control. *International Organization* [online]. 1992, **46**(1), 101-145 [cit. 2018-05-11]. Dostupné z: http://www.jstor.org/stable/2706953
2) CFR. Why Are There No Cyber Arms Control Agreements?. *Council on Foreign Relations: Net Politics and Digital and Cyberspace Policy Program* [online]. 2018 [cit. 2018-05-09]. Dostupné z: https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements
3) DEIBERT, Ronald. Tracking the emerging arms race in cyberspace. *Bulletin of the Atomic Scientists* [online]. 2015, **67**(1), 1-8 [cit. 2018-04-30]. DOI: 10.1177/0096340210393703. Dostupné z: http://www.tandfonline.com/doi/full/10.1177/0096340210393703
4) DEWAR, Robert S. Active Cyber Defense. *ETH Zurich Research Collection* [online]. 2017 [cit. 2018-05-11]. DOI: 10.3929/ethz-b-000169631. Dostupné z: https://www.research-collection.ethz.ch/handle/20.500.11850/181743
5) FINNEMORE, Martha a Kathryn SIKKINK. International Norm Dynamics and Political Change. *International Organization* [online]. **52**(4), 887-917 [cit. 2018-04-15]. DOI: 10.1162/002081898550789. Dostupné z: http://journals.cambridge.org/abstract_S0020818398440608
6) JENSEN, Eric Talbot. Cyber Deterrence. *Emory International Law Review* [online]. 2012, **26**(2), 773-824 [cit. 2018-05-07]. Dostupné z: http://heinonline.org/HOL/P?h=hein.journals/emint26&i=783
7) LEGRO, Jeffrey W. Which norms matter? Revisiting the "failure" of internationalism. *International Organization* [online]. 1997, **51**(1) [cit. 2018-05-08]. Dostupné z: http://www.jstor.org/stable/2703951
8) LESSIG, Lawrence. The Regulation of Social Meaning. *University of Chicago Law Review*. 1995, **62**(1), 943-1046 [cit. 2018-05-09]. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/uclr62&i=947
9) LUPOVICI, Amir. The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives* [online]. 2014, **17**(3) [cit. 2018-05-07]. DOI: 10.1111/insp.12082. Dostupné z: http://isp.oxfordjournals.org/cgi/doi/10.1111/insp.12082
10) MAZANEC, Brian M. Towards a Cyber War Taboo? A Framework to Explain the Emergence of Norms for the Use of Force in Cyberspace. *National Cybersecurity Institute Journal*. 2014, **1**(1), 48-55 [cit. 2018-05-11]. Dostupné z: http://publications.excelsior.edu/publications/NCI_Journal/1-1/offline/download.pdf
11) ROSAMOND, Ben. The uniting of Europe and the foundation of EU studies: Revisiting the neofunctionalism of Ernst B. Haas. *Journal of European Public Policy* [online]. 2005, **12**(2), 237-254 [cit. 2018-04-15]. DOI: 10.1080/13501760500043928. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/13501760500043928
12) SAGAN, Scott D. a Jeremi SURI. The Madman Nuclear Alert: Secrecy, Signaling, and Safety in October 1969. *International Security* [online]. 2003, **27**(4), 150-183. DOI: 10.1162/016228803321951126. Dostupné z: http://www.mitpressjournals.org/doi/10.1162/016228803321951126

13) STEVENS, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy* [online]. 2012, **33**(1), 148-170 [cit. 2018-04-24]. DOI: 10.1080/13523260.2012.659597. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/13523260.2012.659597

14) TANNENWALD, Nina. The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. *International Organization* [online]. **53**(3), 433-468 [cit. 2018-04-15]. DOI: 10.1162/002081899550959. Dostupné z: http://journals.cambridge.org/abstract_S0020818399440779

Monografie

1) BŘÍZA, Vlastislav. *Kontrola, regulace a úprava jaderného zbrojení*. Praha: Karolinum, 2010. ISBN 978-802-4618-647.

2) MAZANEC, Brian M. *The evolution of cyber war: international norms for emerging-technology weapons*. Lincoln: Potomac Books, an imprint of the University of Nebraska Press, 2015. ISBN 978-1612347639.

3) REVERON, Derek S., ed. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Washington, DC: Georgetown University Press, 2012. ISBN 978-158-9019-188.

4) RID, Thomas. *Cyber war will not take place: threats, opportunities, and power in a virtual world*. New York: Oxford University Press, 2013. ISBN 978-0199330638.

Primární zdroje

1) Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. *Office of the Director of National Intelligence* [online]. 2017 [cit. 2018-05-07]. Dostupné z: https://www.dni.gov/files/documents/ICA_2017_01.pdf

2) BARUCH, Bernard. The Baruch Plan: (Presented to the United Nations Atomic Energy Commission, June 14, 1946). *Atomic Archive Library* [online]. 1946 [cit. 2018-05-11]. Dostupné z: http://www.atomicarchive.com/Docs/Deterrence/BaruchPlan.shtml

3) Charter of the United Nations. *United Nations* [online]. 1945 [cit. 2018-05-11]. Dostupné z: http://www.un.org/en/charter-united-nations/

4) CLAPPER, James R. Worldwide Threat Assessment of the US Intelligence Community. In: *Office of the Director of National Intelligence* [online]. 2013 [cit. 2018-04-18]. Dostupné z: https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf

5) CLINTON, Hillary. Secretary Clinton Speaks on Internet Freedom. *YouTube.com: U.S. Department of State* [online]. [cit. 2018-05-11]. Dostupné z: https://www.youtube.com/watch?v=ccGzOJHE1rw

6) Convention on Cybercrime. *Council of Europe Treaty Office* [online]. 2001 [cit. 2018-04-24]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

7) CORRERA, Gordon. How France's TV5 was almost destroyed by 'Russian hackers'. In: *BBC* [online]. 2016 [cit. 2018-04-27]. Dostupné z: http://www.bbc.com/news/technology-37590375

8) Critical National Infrastructure. *Center for Protection of National Infrastructure* [online]. [cit. 2018-04-26]. Dostupné z: https://www.cpni.gov.uk/critical-national-infrastructure-0

9) Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. *Department of Homeland Security* [online]. 2009 [cit. 2018-04-24]. Dostupné z: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

10) International Strategy for Cyberspace. *Obama White House Archive* [online]. 2011 [cit. 2018-05-07]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

11) Joint Publication 3-13: Information Operations. *Department of Defense.* [online]. 2006 [cit. 2018-04-18]. Dostupné z: https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

12) Korea 1952-1954: Document 427. In: KEEFER, Edward C. a John P. GLENNON. *Foreign Relations of the United States: Volume XV, Part 1* [online]. Washington: Government Printing Office, 1984 [cit. 2018-05-10]. Dostupné z: https://history.state.gov/historicaldocuments/frus1952-54v15p1

13) Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. *United Nations Disarmament Reference Library* [online]. 2011 [cit. 2018-04-24]. Dostupné z: https://disarmament-library.un.org/UNODA/Library.nsf/f446fe4c20839e50852578790055e729/329f71777f4b4e4e85257a7f005db45a/$FILE/A-66-359.pdf

14) Quadrennial Defense Review Report. *Department of Defense* [online]. Washington, 2010 [cit. 2018-04-16]. Dostupné z: https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf

15) Seoul Framework. *Data Security Council of India* [online]. 2013 [cit. 2018-04-27]. Dostupné z: https://www.dsci.in/sites/default/files/Seoul%20Framework.pdf

16) The DoD Cyber Strategy. In: *Department of Defense* [online]. 2015 [cit. 2018-05-07]. Dostupné z: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

17) TRUMAN, Harry S. Statement by the President Announcing the Use of the A-bomb at Hiroshima. *The American Presidency Project* [online]. 1945 [cit. 2018-04-15]. Dostupné z: http://www.presidency.ucsb.edu/ws/?pid=12169

18) Trump: Claims of Russian interference in 2016 race 'ridiculous,' Dems making excuses. *Fox News Politics: Trump Transition* [online]. 2016 [cit. 2018-05-09]. Dostupné z: http://www.foxnews.com/politics/2016/12/11/trump-claims-russian-interference-in-2016-race-ridiculous-dems-making-excuses.html