VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA MEZINÁRODNÍCH VZTAHŮ

DIPLOMOVÁ PRÁCE

2015 Veronika Fleischmannová

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

Fakulta mezinárodních vztahů

Hlavní specializace: Mezinárodní politika a diplomacie

Kybernetická bezpečnost

Diplomová práce

Vypracovala: Bc. Veronika Fleischmannová

Vedoucí diplomové práce: Ing. PhDr. Radka Havlová, Ph.D.

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma *„Kybernetická bezpečnost“* vypracovala samostatně. Veškerou použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

V Praze dne 27. dubna 2015

.....

Podpis

Poděkování

Ráda bych touto cestou upřímně poděkovala Ing. PhDr. Radce Havlové, Ph.D. za všechny připomínky, podněty a čas, který mi věnovala během konzultací a vedení mé diplomové práce.

Obsah

Seznam zkratek

A2/AD	Anti-Access/Area Denial
CICIR	China Institutes of Contemporary International Relations
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CNA	Computer network attack
CND	Computer network defense
CNE	Computer network exploitation
CNO	Computer network operations
CYBERCOM US	Cyber Command
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
GGE	Group of Government Experts
ICS	Industrial control system
ICT	Information and Communications Technology
IO	Information Operations
IT	Information Technology
IPTV	Televize přes internetový protokol
IRC	Internet Relay Chat
ISO	Information Security Standard
ITRs	International Telecommunication Regulations
ITU	International Telecommunications Union
IW	Information Warfare
MTR	Military-Technical Revolution
NATO	North Atlantic Treaty Organisation
NCO (W)	Network Centred Operations (Warfare)
NSA	National Security Agency
RAND	Research and Development – Corporation
RMA	Revolution in Military Affairs
WCIT-12	World Conference on International Telecommunications (2012)

Úvod

Současné mezinárodní prostředí je z velké části formované procesy globalizace a následkem tohoto dynamického procesu velmi proměnlivé. Globalizace prostupuje všechny obory lidské existence (ekonomické, politické, kulturní a sociální), odstraňuje bariéry, propojuje jednotlivé státy i regiony bez ohledu na hranice. Vývoj lidské společnosti je v současné době těsně svázán s kyberprostorem a potažmo s internetem, se kterým se snažíme kyberprostor ztotožnit. 21. století je stoletím informačních technologií. Informační a komunikační technologie jsou využívány při finančních transakcích, komunikaci, obchodních aktivitách, ve zdravotnictví, primárním výzkumu, ale i v mnoha dalších oblastech lidské činnosti. Internet hraje klíčovou roli v našem každodenním životě, ekonomice a bezpečnosti. Dochází zde k přenosu obrovského množství a ukládání dat, komunikaci, finančním transakcím, komerčním aktivitám, vědeckému výzkumu, a dokonce jsou informační a komunikační technologie využívány při vojenských operacích. Globální ekonomika díky internetu zažívá nebývalý rozkvět. Pro rozvojové země představují informační a komunikační technologie dokonce hnací motor jejich rozvoje. Více než 2,5 miliard[1] zákazníků nakupuje zboží a služby a provádí elektronické platby přes internet. Počet internetových uživatelů na celém světě překračuje 3 mld. a od roku 2000 stoupl o 741%.[2]

Charakteristické vlastnosti kyberprostoru a potažmo internetu, jako je jeho otevřenost, relativní anonymita, neomezené hranice vstupu, globální působnost a propojenost a především decentralizace, z něj dělá nový cíl útoků a vytváří prostor pro kriminalitu. Kyberprostor rovněž přináší fenomén kyberválky jakožto novou podobu konfliktu. Ekonomická, sociální, politická a technologická závislost na internetu je natolik vysoká, že jeho ochrana se stala prioritou každého státu. Zásadním problémem výzkumu kyberprostoru a kybernetické bezpečnosti je absence mezinárodního režimu, který by univerzálně upravoval a definoval základní pojmosloví a otázky kybernetické bezpečnosti; tato problematika byla doposud řešena pouze na úrovni jednotlivých států. Nevyhnutelná potřeba mezinárodně ukotvit kybernetický prostor, a především koncept užití síly v něm, vychází z předpokladu, že státy považují kyberprostor za pátou válečnou doménu. Za zásadní překážku v sestavení mezinárodních norem pro oblast kybernetické bezpečnosti lze pokládat to, že aktivity

[1] KLIMBURG A. (ed.). *National Cyber Security Manual*, 2012: str.3

[2] Internet World Stats. *World Internet Users and 2014 Population Stats,* 2014

prováděné na internetu se uskutečňují mimo kontrolu států a nezáleží na tom, jak mocný stát je.

Diplomová práce se proto snaží přiblížit problematiku kybernetické bezpečnosti a nový fenomén kybernetických hrozeb, které ohrožují nejenom samotný stát, ale kybernetická kriminalita se může dotýkat i běžného internetového uživatele. Globální charakter kyberprostoru a spojitá světová síť internet, neomezená státními hranicemi, přispívá k tomu, že veškeré aktivity – legální i nelegální – se obtížně lokalizují.

Předmětem zkoumání diplomové práce bude koncept kybernetické bezpečnosti a kybernetických hrozeb jako nového fenoménu, který ohrožuje národní bezpečnost. Problematika bude podrobněji vysvětlena v případové studii dokumentující spory mezi Čínou a USA v kyberprostoru.

Cílem mé práce bude ověření hypotézy, že mezi Čínou a Spojenými státy probíhá kybernetická válka. Metody, které povedou k tomuto cíli, budou vycházet ze studia poznatků z odborné, především cizojazyčné literatury. Základem bude analýza informací z odborných textů a komparace různých náhledů na danou problematiku. Nejdříve bude porovnán přístup pozorovaných zemí k problematice kybernetické bezpečnosti a následně bude teoretický rámec kybernetické bezpečnosti aplikován na konkrétní případy.

Práce se skládá ze dvou částí, teoretické a analytické. Teoretická část je vymezena v prvních dvou kapitolách. Kapitola první se zabývá proměnou bezpečnostního prostředí 21. století a konceptem bezpečnosti Kodaňské školy. Následující podkapitola 1.2 „Vojensko-technická revoluce, revoluce ve vojenských záležitostech a informační revoluce“ popisuje transformaci vojenství a společnosti v závislosti na informačních a komunikačních technologiích. Informace se stává strategickou a hodnotnou veličinou. V následujících třech podkapitolách jsou definovány pojmy kyberprostor, kybernetická bezpečnost a rozvedeno pět dilemat kybernetické bezpečnosti. Obsahem druhé kapitoly je kvalifikace kybernetických hrozeb na základě motivu a prostředků útočníka, mezi něž patří kybernetická špionáž, kyberválka, kyberzločin a kyberterorismus. Kapitola 2.2 analyzuje dosažené pokroky v sestavení závazných pravidel upravujících kyberprostor v rámci mezinárodní spolupráce.

Analytická část diplomové práce se zabývá případovou studií sporů mezi Čínou a USA v oblasti kyberprostoru. Nejdříve jsou vysvětleny a porovnány přístupy obou zemí k oblasti kybernetické bezpečnosti a spolupráce na bilaterární úrovni týkající se této problematiky. Poslední kapitola analyzuje americko-čínskou leteckou kolizi následující hackerskou válkou a dopad incidentu na vzájemné vztahy. A v neposlední řadě jsou

studovány kybernetické špionážní aktivity Číny proti americkým cílům a následná reakce americké vlády na tyto aktivity.

Studium kybernetické bezpečnosti představuje nový multidisciplinární obor na pomezí informatiky, práva, bezpečnostních studií a mezinárodních vztahů. Protože se dostává problematika kybernetické bezpečnosti a její dílčí segmenty do popředí zájmu nejen odborné, ale i laické veřejnosti a médií, vznikla od počátku milénia celá řada prací, které téma z různých úhlů zkoumají. Stěžejními zdroji pro teoretické ukotvení problematiky kybernetické bezpečnosti se staly především National Cyber Security Framework Manual a dále tzv. Tallinnský manuál či národní strategie pro kybernetickou bezpečnost (například manuály USA, Číny a Velké Británie nebo České republiky), které vymezují danou problematiku pro vnitrostátní potřebu. Z hlediska mezinárodního práva je rovněž klíčová Úmluva o kyberzločinu zaštítěná Radou Evropy. Tento dokument představuje první mezinárodněprávní dokument určený k řešení problémů v oblasti počítačového zločinu s mezinárodním přesahem. Výše uvedené prameny povětšinou pokládají kybernetickou hrozbu za asymetrický druh nebezpečí, kterými útočí jednotlivci či malé skupiny na soukromé subjekty a složky státní moci. Pojem kyberválky jakožto symetrického konfliktu států mezi sebou zavádí analýza Cyberwar is comming!, za níž stojí autoři z think-thanku RAND. V českém prostředí problematiku studuje například Václav Jirovský, autor publikace Kybernetická kriminalita, z níž tato práce také vychází.

Případová studie je opřena především o informace z webových stránek amerických federálních a čínských institucí, oficiálních dokumentů a dále pak čerpá z článků zahraničních zpravodajských webů, dokumentujících jednotlivé incidenty kybernetické bezpečnosti mezi lety 2000 až 2014. Mezi nejvýznamnější prameny případové studie lze zařadit také stať Cyber Warfare and Sino-American Crisis Instability.

Překážkou při zpracování případové studie byla poměrně značná absence oficiálních čínských stanovisek či analýz domácích, čínských autorů. Příčinou je jednak jazyková bariéra, neboť ne všechny zdroje jsou přístupné v anglickém překladu, jednak obecná disproporce v objemu vydaných západních a čínských písemných materiálů. Čínští autoři, z jejichž závěrů práce také vychází, píší již povětšinou v angličtině a žijí mimo území Číny.

1 Bezpečnostní prostředí 21. století

Konec studené války a s ním postupující eroze bipolárního mezinárodního prostředí a zrychlující se globalizační procesy spolu s nástupem globální civilizace výrazně oživily úvahy o novém bezpečnostním rámci, který by adekvátně reagoval na výzvy a hrozby 21. století. Nejvýraznější příspěvek do diskuze o novém konceptu národní bezpečnosti představuje tzv. rozšířené pojetí bezpečnosti Kodaňské školy a jejích hlavních představitelů B. Buzana a O. Waevra. Široké pojetí bezpečnosti Kodaňské školy se vyznačuje akceptací většího počtu aktérů a různorodých bezpečnostních témat. Bezpečnostní hrozby nemají pouze vojenský charakter, jak tomu bylo u klasických realistických autorů. Hrozby mohou vycházet jak z politické, ekonomické, environmentální, tak societální oblasti (tzv. sektorů). Buzanova bezpečnostní analýza rovněž opouští státocentrický pohled ve prospěch sociálních skupin. Přístup Kodaňské školy ke konceptu bezpečnosti odráží posun od státocentrického realistického konceptu národní bezpečnosti k mezinárodní bezpečnosti reagující na globalizující se rozmanité prostředí.[3]

Vojenské konflikty rovněž prošly jistou transformací – rozsáhlé mezistátní vojenské války setrvale klesají a války 21. století jsou převážně válkami mezi nestátními aktéry, popřípadě mezi státem a nestátními aktéry.[4] Kyberprostor dává současným konfliktům zcela nový rozměr. V rámci mezinárodní diskuze se rozvíjí koncept kyberprostoru coby páté válečné domény. Zásadní vojenský význam kyberprostoru spočívá v rostoucí míře využívání pokročilých technologií pro vojenské účely. Vysoká závislost společnosti na informačních a komunikačních technologiích s sebou přináší i různá rizika. Poměrně neomezený přístup k internetu a relativní anonymita, kterou poskytuje, vytváří z kyberprostoru nový cíl a zároveň nástroj útoků. Nejzranitelnější je závislost kritické infrastruktury státu na kyberprostoru, neboť této zranitelnosti může využít nepřítel k získání strategické výhody. Úspěšně provedený útok například na kritickou informační infrastrukturu[5] může mít za následek destabilizaci států.

---

[3] WAISOVÁ, Š. *Od národní bezpecnosti k mezinárodní bezpecnosti,* 2004: str. 67

[4] NYE, J. *Is Military Power Becoming Obsolete?*, 2010

[5] Kritická informačí infrastruktura států představuje komplex informačních a komunikačních systémů a jejich služeb, sloužící k informačnímu zajištění řádné funkčnosti kritické infrastruktury. Sestává z částí, jakými jsou telekomunikace, počítačové systémy a jejich programové vybavení, Internet, přenosové sítě, poskytované služby atd.

1.1 Rozšířené pojetí bezpečnosti – Kodaňská škola

Kodaňská konceptualizace bezpečnosti představuje jeden z nejvlivnějších současných přístupů k výzkumu bezpečnosti. Ukazuje proměnu realistického konceptu národní bezpečnosti a vytvoření nového konceptu bezpečnosti rozšířeného o nové jevy reflektující situaci po konci studené války. Barry Buzan přijal myšlenku existence mezinárodní společnosti (koncept tzv. Anglické školy), která vytváří sociální prostředí, v němž se státy pohybují a spolupracují na základě sdílených institucí. Myšlenka mezinárodní společnosti vede k částečnému překonání anarchie mezinárodního systému a umožnila Buzanovy uvažovat o proměně bezpečnostních vztahů mezi státy. Kodaňská škola se rovněž odklání od objektivního pojetí bezpečnosti a definuje bezpečnost jako subjektivní proměnnou. Bezpečnost jako subjektivní proměnná závisí na sociálním prostředí, na vnímání hrozeb a jejich interpretaci. Ze základu studia vnímání a interpretace hrozeb vychází analýza sekuritizace, kdy se určité téma stává bezpečnostním problémem nikoli v důsledku objektivní hrozby, ale proto, že je jako hrozba definováno například vládou či významnou mezinárodní organizací a společnost tuto definici hrozby přijme.[6]

Koncept bezpečnosti podle Kodaňské školy se pohybuje po dvou osách: vertikální a horizontální. Osa vertikální obsahuje referenční objekty – aktéry, kteří jsou existenčně ohroženi. Mezi ně patří jedinec, vnitrostátní skupiny, stát, regionální a mezinárodní systém. Horizontální osa představuje sektorovou logiku konceptu bezpečnosti. Mezi sektory panují dynamické vztahy a vzájemná interakce. Sektorová logika přispívá k uvědomění si složitosti současné bezpečností reality a zároveň umožňuje její zjednodušení pro účely zkoumání.[7]

Podle Kodaňské školy představuje bezpečnost zvláštní typ politiky, jejíž dynamika a charakter jsou zkoumány v pěti klíčových sektorech – vojenství, politika, ekonomika, životní prostředí a společnost. Každý sektor obsahuje odlišné zdroje hrozeb. Úlohu jednotlivých sektorů vysvětluje Buzan následovně[8]:

---

[6] WAISOVÁ, Š. *Od národní bezpecnosti k mezinárodní bezpecnosti,* 2004: str. 67

[7] WAISOVÁ, Š. *Od národní bezpecnosti k mezinárodní bezpecnosti,* 2004: str. 72

[8] BUZAN, B. *People, States and Fear*, 1991, str. 20-21. In: BUZAN, B. a kol. *Bezpečnost, Nový rámec pro analýzu*, 2005: str. 17.

Vojenský sektor bezpečnosti obsahuje tradiční hrozby, které se dotýkají zejména vnější a vnitřní státní suverenity. Jedná se o vzájemné působení ofenzivních a defenzivních schopností států a dále i to, jak státy vnímají úmysly a záměry ostatních.

Politický sektor popisuje vztahy autorit a zahrnuje organizační stabilitu států, systémy vládnutí a ideologie, které slouží pro jejich legitimitu.

Ekonomickým sektorem bezpečnosti rozumíme přístup ke zdrojům, finančním prostředkům a trhům, bez nichž nelze udržet přijatelnou životní úroveň a dostatečnou státní moc. Silná ekonomika státu je nezbytnou podmínkou pro budování finančně náročné vojenské základny státu. Celá řada hrozeb je důsledkem výrazné vzájemné ekonomické závislosti a provázanosti, která je charakteristická pro současnou globalizující se ekonomiku.

Zdroje hrozeb pocházející ze společenského sektoru se dotýkají identit větších sociálních skupin, jakými jsou nejen národy, ale i jinak etnicky, kulturně, rasově či nábožensky definované skupiny. Jedná se například o uchování tradičních forem jazyka, kultury, náboženství a národní identity v procesu vývoje. Typickými hrozbami pro společenský sektor jsou migrace, nacionalismus, rychlý populační růst či prohlubující se rozdíl mezi Severem a Jihem.

Environmentální sektor se týká zachování lokální i celoplanetární biosféry coby základního podpůrného systému, na němž závisí existence všech dalších forem lidské činnosti. Zdroje hrozeb, charakteristické pro tento sektor, souvisí se zásahy způsobujícími změny životního prostředí, šíření epidemií, obchodování se vzácnými zvířaty a rostlinami nebo přírodní katastrofy.

Základních pět sektorů Kodaňské školy rozšíříme o jeden další a zavedeme nový pojem kybernetický sektor[9]. Rozšíření konceptu lze chápat jako nezbytný předpoklad pro systematickou analýzu kybernetické bezpečnosti. Jevy, jež kybernetický sektor zahrnuje, prostupují všemi pěti tradičními sektory a jsou determinovány jejich aktéry. Kybernetický sektor tedy určitým způsobem propojuje ostatních pět sektorů a zjednodušuje popis vztahů mezi aktéry v kyberprostoru. Kybernetický sektor bezpečnosti popisuje ochranu informačních systémů, které jsou nutnou podmínkou pro fungování všech lidských aktivit v současném informačním věku. Tradiční interakcí v tomto sektoru je šíření a výměna informací. K nejvýraznějším hrozbám patří vážné narušení kritické infrastruktury státu,

[9] Kybernetickým sektorem a kybernetickou bezpečnosti se v rámci teorie sekuritizace zabývají Lene Hansen a Helen Nissenbaum v článku *Digital Disaster, Cyber Security, and the Copenhagen School* (2009) v International Studies Quarterly.

kyberšpionáž, krádež tajných informací, obchodních tajemství, duchovního vlastnictví, hacktivismus[10], kybernetické útoky následující ozbrojeným útokem.

Ačkoliv bylo řečeno, že kybernetický sektor není zaveden jako všeobecně uznávaný pojem v terminologii Kodaňské školy a jedná se spíše o sumu vybraných jevů, které se týkají kybernetické bezpečnosti a jejích aktérů, z hlediska současného významu informačních a komunikačních technologií jej však můžeme považovat za svébytnou jednotku.

Výčet referenčních objektů, ohrožených hodnot a zdrojů hrozeb v jednotlivých sektorech je obsahem následující tabulky.

Tabulka 1 – Rozšířený koncept bezpečnosti

Sektory (zdroje hrozeb)	Referenční objekty	Ohrožené hodnoty	Zdroje hrozeb
Vojenský	Státy, ozbrojené síly	Suverenita, územní celistvost	Státy, vnitrostátní skupiny, příroda
Environmentální	Životní prostředí, ekosystém, lidstvo	Udržitelnost, kvalita života	Lidstvo, státy, globalizace (např. industrializace, doprava)
Ekonomický	Národní ekonomiky, ekonomické režimy, globální ekonomika	Konstitutivní pravidla, normy, instituce (např. liberalismus, volný obchod)	Globální ekonomika, firmy (např. TNK)
Společenský	Národy, společenské skupiny (např. etnické, náboženské)	Kolektivní identita, integrita	Státy, nepřátelské skupiny, globalizace (např. migrace, kulturní homogenizace)
Politický	Státy, mezinárodní organizace, režimy, společenství	Konstitutivní pravidla, normy, instituce (např. státní ideologie, idea integrace)	Státy, globalizace
Kybernetický	Státy, kritická infrastruktura, informační komunikační technologie, internet a sociální sítě	Důvěrnost, dostupnost a integrita informací	Státy, jednotlivci - hackeři, nepřátelské skupiny (např. hacktivisté)

Vytvořeno podle LEHMANNOVÁ, Z. *Formování globálního řádu? Globalizace a global governance*, 2010: s. 117. Vlastní úpravy autorky.

[10] Hactivismus představuje politicky a ideově motivovaný hacking.

1.2 Vojensko-technická revoluce, revoluce ve vojenských záležitostech a informační revoluce

Vojenské kapacity, doktríny a strategie se nepřetržitě vyvíjí v závislosti na technologickém rozvoji. Tento neustále probíhající proces ve vojenství, využívající nových vědeckých poznatků, se nazývá „Revoluce ve vojenství“ (Revolution in Military Affairs, RMA). Problematikou revoluce ve vojenství se poprvé zabývali sovětští stratégové v 70. a 80. letech 20. století. Postupně se mluví o konceptu tzv. vojensko-technická revoluce (Military-Technical Revolution, MTR). Za protagonistu tohoto konceptu je označován maršál Nikolaj V. Ogarkov zabývající se zejména rozvojem nových technologií ve vojenství (například přesně naváděná munice, nenukleární zbraně). Dle Ogarkova se tyto změny projevují nejen v nárůstu počtu nukleárních zbraní, ale povedou také k transformaci tradičního způsobu vedení boje. Myšlenky MTR dále rozvíjí američtí analytici; poukazují přitom na výlučně technologický rozměr konceptu a nabízejí více holistický koncept „revoluce ve vojenských záležitostech“ (Revolutions in Military Affairs, RMA).[11]

Teoretici došli k závěru, že RMA dramaticky ovlivnila efektivnost vedení boje, a to zejména díky technologické změně, rozvoji systémů, operačním inovacím a organizační adaptaci.[12]

21. století je stoletím informačních technologií. V důsledku proměny moderní společnosti se informace stává strategickou a hodnotnou veličinou. Způsob vedení boje již není založen na tom, kdo disponuje největším počtem vojáků, kapitálu, či nejmodernějšími technologiemi, ale především na tom, kdo má nejlepší informace o bojišti.[13] Informační revoluce se stává hnacím motorem současné společnosti a zásadním způsobem proměňuje podstatu moci. Důsledkem enormního poklesu transakčních nákladů spojených s přenosem informací a rozvojem moderních informačních technologií je šíření informací mnohem jednodušší a rychlejší. Informační revoluce překračuje pomyslné hranice a redistribuuje moc v takovém měřítku, že světová politika přestává být pod výlučnou dominancí vlád. Přímo se

[11] FUČÍK, J., KŘÍŽ, Z. *Informační revoluce, vojensko-technická revoluce, nebo revoluce ve vojenských záležitostech?*, 2013

[12] Tamtéž.

[13] ARQUILLA, J., RONFELDTSTR, D. *Cyberwar is coming*!, 1993: str. 23

zapojují jednotlivci či soukromé organizace – jako například WikiLeaks, nevládní organizace, nadnárodní korporace, teroristické skupiny či různá sociální hnutí.[14]

Následkem informační revoluce dochází k erozi tradičních hierarchických struktur, na jejichž základě jsou instituce vytvořeny, a naopak umocňuje důležitost všech forem síťového uspořádání – například komunikačních či sociálních a zvláště pak multiorganizačních sítí. Rozdíl mezi hierarchickým uspořádáním velkých institucí a multiorganizačních sítí spočívá v jejich jednání. Zatímco velké instituce jednají na vlastní pěst, multiorganizační sítě se skládají z více menších organizací či částí institucí, které jednají společně. Moderní informační a komunikační systémy zefektivnily aktivity každodenního života společnosti, ale také vytváří prostor pro nové hrozby spojené s informační revolucí.[15]

1.3 Kyberprostor a jeho význam

Pojem „cyber“, úzce spojovaný s počítači a sítěmi, je často medializován a to především co se týče bezpečnostních záležitostí. Pojetí kybernetiky rozvinul Norbert Wiener ve svém díle z roku 1948: *Kybernetika aneb Řízení a sdělování u organismů a strojů (Cybernetics: Or Control and Communication in the Animal and the Machine)*. Následkem toho, že stroje mohou rozšířit lidské schopnosti, se vytváří alternativní prostředí interakce mezi člověkem a strojem, které položilo základy konceptu kyberprostoru. Termín kyberprostor poprvé použil americký spisovatel William Gibson a zpopularizoval ve své knize *Neuromancer (1984)*, čímž se rázem přenesl i do profesionálních a akademických kruhů. Gibsnův kyberprostor přestavuje: *„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost.“*[16] Gibsonova definice se zaměřuje na bezprostřední lidské vnímání kyberprostoru a na základní princip, jímž je komplexnost.

Podle Mezinárodní organizace pro normalizaci (The International Organisation for Standardisation – ISO) kyberprostor lze definovat jako *„technologicky a síťově vytvářené*

[14] NYE, J. *The Information Revolution Gets Political*, 2013

[15] ARQUILLA, J., RONFELDTSTR, D. *Cyberwar is coming*!, 1993: str. 27

[16] SINGER, P. *Cybersecurity and Cyberwar: What everyone need to know*. 2014: str. 12

komplexní prostředí vycházející z interakce lidí, softwaru a internetových služeb, které neexistuje v jakékoliv fyzické formě". [17]

Každý stát si vytváří svoji vlastní definici kyberprostoru, kterou promítne do své národní kybernetické bezpečnostní strategie. Například definice kyberprostoru amerického ministerstva obrany je následující: „*Kyberprostor představuje globální prostředí tvořené infrastrukturou informačních technologií zahrnující internet, telekomunikační sítě, počítačové systémy, procesory a řídící jednotky (Joint Publication 1-02).*"[18] Tato definice se příliš omezuje na digitální pevné komponenty a nejenomže postrádá lidský prvek jak tomu bylo u Gibsonova či Wienerova pojetí kyberprostoru, ale současně opomíjí reflektovat rozsáhlé dynamické, technologické či sociální změny, se kterými je kyberprostor svázán.[19] Podrobněji se budeme zabývat americkou kybernetickou bezpečností strategií v další kapitole.

Spojené království pojímá kyberprostor jako *„jakékoliv formy síťových a digitálních aktivit, tento pak zahrnuje jak obsah, tak činnosti prováděné přes digitální sítě"*.[20] Státy tak můžou posuzovat jakékoliv chování na internetu jako přijatelné či nepřípustné. Lidé považují internet za prostor, kde se mohou svobodně vyjádřit, a tudíž jakákoliv cenzura internetu může být vnímána jako narušení tohoto práva. Internet je předmětem ochrany před kriminalitou, špionáží, terorismem a jakékoliv formy válčení.[21]

Na rozdíl od západních zdrojů, kde je na kyberprostor nahlíženo jako na samostatnou doménu, Čína pojímá kyberprostor jako pouhou součást informačního prostoru. Informační prostor pak představuje *„prostor pro vzájemnou komunikaci mezi lidmi, který je integrací celosvětové komunikační sítě, databází a informací, vytváří obrovskou propojenou "krajinu", kde mohou interagovat různé etnické nebo rasové skupiny a tvoří tak trojrozměrný prostor."*[22] Nejbližším termínem pro kyberprostor je pak pojem webový server jako *„nezbytné*

---

[17] ISO/IEC 27032, *Information technology — Security techniques — Guidelines for cybersecurity*, 2012

[18] OTTIS, R., LORENTS, P. *Cyberspace: Definition and Implications*, 2012

[19] KUEHL D. From Cyberspace to Cyberpower. Defining the Problem, 2009: str. 2

[20] UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space*, 2009

[21] Tamtéž.

[22] WASUO, H. B. *Information Space*, 2000. *In*: GILES, K. *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*, 2013

komponenty pro připojení přístroje k síti za účelem komunikace přes protokoly HTML, email a další.“[23]

Ottis a Lorents nabízí tuto definici: „*Kyberprostor představuje množinu vzájemně provázaných informačních systémů závislých na čase a jejich uživatelích.*“[24] Tato definice určuje jednak dynamičnost kyberprostoru, jednak obsahuje lidský prvek, neboť kyberprostor je uměle vytvořené rozhraní vytvořené člověkem pro jeho potřeby. Bez lidské činnosti by kyberprostor mohl stagnovat, či upadnout do chaosu nebo dokonce přestat existovat, a tudíž se člověk stává neodmyslitelnou součástí kyberprostoru. Vzhledem k provázanosti informačních systémů se dramatické změny mohou promítnout v relativně krátkém čase. Příkladem může být zásah škodlivého kódu, který se dokáže během několika sekund či minut sám replikovat a efektivně vyřadit z činnosti světovou síť.

„Kritické informační infrastruktury (Critical information infrastructures – CII) zahrnují vzájemně provázené informační systémy a sítě, narušení či zničení těchto systémů a sítí by mělo vážné dopady na zdraví, na zajištění bezpečnosti, blahobyt obyvatelstva či efektivní fungování vlády či ekonomiky.“ [25] Národní CII většinou zahrnují alespoň některé z následujících prvků:

- Informační komponenty podporující kritickou infrastrukturu;
- informační infrastrukturu podporující základní prvky vládní činnosti;
- informační infrastrukturu nezbytnou pro národní ekonomiku.

Z definice CII můžeme vyvodit závěr, že napadení jakékoliv národní CII můžeme považovat za akt války. Kyberprostor nelze zjednodušit pouze na internet, hardware, software a informační systémy, ale musíme do něj zahrnout i lidský prvek a sociální interakce, které probíhají právě v rámci počítačové sítě.

Současným vzrůstajícím trendem v kyberprostoru jsou nelegální a nekalé praktiky získávání informací a průmyslová špionáž velkých obchodních společností, organizací a vlád. Napomáhá tomu i fakt, že ICT poskytují relativní anonymitu a konkrétního pachatele lze těžce vypátrat. Dalším faktorem, který přispívá k provádění těchto nezákonných aktivit, je

---

[23] WASUO, H. B. *Information Space*, 2000. *In*: GILES, K. *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*, 2013

[24] OTTIS, R., LORENTS, P. *Cyberspace: Definition and Implications*, 2012

[25] OECD. *Recommendation of the Council on the Protection of Critical Information Infrastructures,* 2008: str. 4

skutečnost, že podobné operace nevyžadují žádné vysoké profesionální ani finanční požadavky či vyspělou průmyslovou základnu. Počítačové červy[26] jako je například Stuxnet, Flame a Duqu dokáží proniknout do vzdálených počítačových systémů a následně je pak ovládat. Nejčastějším počítačovým programem určeným ke vniknutí do počítačového systému je malware[27]. Podle americké společnosti Symantec bylo v roce 2011 identifikováno přes 400 miliónů druhů malwaru, které zcizily obchodní, soukromá a tajná data. Mezi nejčastější oběti těchto útoků patří nadnárodní obchodní společnosti, jmenujme například firmy Sony, Yahoo, Citigroup, Linked-In a další.[28]

1.4 Kybermoc

Kybermoc (Cyberpower) můžeme definovat jako *„schopnost dosáhnout svých cílů prostřednictvím využití moderních informačních technologií, a to i mimo kyberprostor.“*[29] Kramer pojímá cyberpower především z vojenského hlediska jako *„schopnost využít výhod kyberprostoru k ovlivnění událostí ve všech operačních prostředích a napříč nástroji moci.“*[30] Z této definice vyplývá jednoznačné chápání kyberprostoru jako vojenského operačního prostředí, srovnatelného se zemským, vzdušným, mořským či vzdušným prostorem. Takto ho pojímá i americká vláda ve své bezpečnostní národní strategii (vysvětleno níže).

Čína patří mezi země s největším počtem internetových uživatelů – v zemi je podle statistik okolo 641 601 070 uživatelů, což představuje 46,03% celkového obyvatelstva[31] a

---

[26] Červ (worm) představuje autonomní program, schopný vytvářet své kopie, které rozesílá do dalších počítačových systému (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

[27] Malware je souhrnný pojem pro jakýkoli software, který při svém spuštení zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštecí událost (např. na okamžik, kdy oprávnený uživatel otevře zprávu v rámci elektronické pošty).

[28] KLIMBURG A. (ed.). *National Cyber Security Manual*, 2012: str. 6

[29] NYE, J. *The Future of Power*, 2001: str. 123

[30] KRAMER, F. *Cyberpower and National Security*, 2009: str. 38

[31] Internet Live Stats. *Internet Users by Country (2014)*, 2014

„stát se kybernetickou mocností patří mezi nejdůležitější součást tzv. Čínského snu“[32]. Spojené státy americké počítají na 279 834 232 internetových uživatelů, což obnáší 86,75% z celkového počtu obyvatel.[33]

1.5 Kybernetická bezpečnost

Agendě kybernetické bezpečnosti se v posledních letech přisuzuje stále zásadnější význam a to zejména v důsledku celosvětového rozvoje informačních a komunikačních technologií ICT. V současné době ICT prostupují celou společností a společnost je na těchto technologiích fakticky závislá. Rostoucí míra závislosti na těchto technologiích a kyberprostoru však s sebou nese kromě výhod také možná rizika a hrozby. Mezi nejdůležitější témata patří ochrana vládních tajemstvích a kritické infrastruktury, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Kyberprostor není omezen státními hranicemi či kontinenty, přístup je takřka neomezený a umožňuje i relativní anonymitu. Vzhledem k těmto vlastnostem se vytváří příznivé prostředí pro kybernetickou kriminalitu. Prostřednictvím internetu dochází například k nelegálnímu obchodu s osobními údaji či jinými citlivými daty, přesměrování plateb, špionáži; skrze různá internetová fóra dochází k propagaci rasismu, extremismu a terorismu.

S kybernetickou bezpečností úzce souvisí informační bezpečnost. *„Informační bezpečnost je multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Jejím cílem je snižování rizik a navrhovat příslušná opatření z hlediska organizačního, řídícího, metodického, technického, právního a dalšího hlediska, související s touto problematikou.“*[34] Většina států klade důraz při formulaci své bezpečnostní kybernetické strategie právě na nutnost zabezpečení informací. Mezi základní principy informační bezpečnosti patří zachování důvěrnosti, integrity a dostupnosti informací. Ústředním zájmem informační

[32] CCTV. *Building networks to achieve power is an important part of Chinese Dream*, 2014

[33] Internet Live Stats. *Internet Users by Country (2014)*, 2014

[34] Ministerstvo vnitra České republiky, *Základní definice, vztahující se k tématu kybernetické bezpecnosti*, 2009

bezpečnosti jsou data a to bez ohledu na jejich formu – elektronickou, tištěnou či jinou. Počítačová bezpečnost má na druhou stranu zajistit dostupnost a bezchybný chod počítačového systému bez ohledu na uložená data.[35]

ISO chápe kybernetickou bezpečnost v kontextu informační bezpečnosti jako *„zachování integrity, dostupnosti a důvěryhodnosti informací v kyberprostoru“*. Zároveň poukazuje na potřebu překlenout mezeru mezi různými bezpečnostními oblastmi, na kterých je současně kybernetická bezpečnost závislá. Jedná se zejména o oblast informační, internetové a síťové bezpečnosti a ochrany kritické informační infrastruktury (CIIP).[36] Kritickou informační infrastrukturu státu tvoří komplex informačních a komunikačních systémů a jejich služeb, sloužící k informačnímu zajištění řádné funkčnosti kritické infrastruktury. Patří sem telekomunikace, počítačové systémy a jejich programové vybavení, Internet, přenosové sítě, poskytované služby atd.[37]

Naopak podle Mezinárodní telekomunikační unie (International Telecommunication Union - ITU) je kybernetická bezpečnost široce definována jako: *„Soubor nástrojů, politik, pokynů, bezpečnostních konceptů, osvědčených postupů, přístupů k řízení rizik, školení a technologií, které jsou zapotřebí k zajištění ochrany kybernetického prostředí, organizací a majeteku běžného uživatele. Organizace a majetek běžného uživatele zahrnují připojená zařízení, personál, infrastrukturu, aplikace, služby, telekomunikační systémy a celkový objem přenesených a/nebo uložených dat. Kybernetická bezpečnost se snaží zachovat a ochránit majetek organizace a uživatele před případnými bezpečnostními riziky pocházejícími z kybernetického prostředí. Mezi hlavní cíle kybernetické bezpečnosti patří: dostupnost, integrita a důvěryhodnost informací.“*[38]

Z vojenského hlediska je kladen důraz na kybernetickou obranu. Kybernetická obrana je chápána v rámci NATO jako *„schopnost zajistit chod a bezpečnost komunikačních a informačních systémů před potenciálními a bezprostředními hrozbami, které pocházejí*

---

[35] KLIMBURG A. (ed.). *National Cyber Security Manual*, 2012: str. 9

[36] ISO/IEC 27032, *Information technology — Security techniques — Guidelines for cybersecurity*, 2012

[37] Ministerstvo vnitra České republiky, *Základní definice, vztahující se k tématu kybernetické bezpecnosti*, 2009

[38] ITU, *Definition of cybersecurity* [online]. 2015 [cit. 25.4.2015]. Dostupné z: http://www.itu.int/

z kyberprostoru".[39] Hovoří se o tom, že až 120 států[40] disponuje kybernetickými zbraněmi a jsou schopné vést kybernetickou válku. Vojenské kybernetické činnosti zahrnují následující úkoly: ochrana vlastních obranných sítí, využití informační technologie k výhodě na bojišti neboli využít schopností Network Centric Warfare (NCW), a nakonec kyberválčení strategické, taktické nebo na bojovém poli.

Cílem kybernetické bezpečnosti je bezpečný kybernetický prostor. Ochrana kritické infrastruktury je důležitým faktorem pro úspěšný rozvoj globální ekonomiky. V oblasti národní kybernetické obrany je nezbytná široká mezinárodní spolupráce, zapojení bezpečnostních institucí a subjektů zabývajícími se vývojem nových technologií. Moc a zodpovědnost je v kyberprostoru roztříštěna mezi rozličné aktéry. Spolupráce při formulování národní kybernetické bezpečnostní strategii je důležitá na třech úrovních: *vládní, národní a mezinárodní*.[41]

1) Spolupráce na vládní úrovni

Vzhledem ke složitosti a komplexnosti kybernetické bezpečnosti je nezbytné, aby mezi sebou spolupracovaly různé rezorty, agentury a jiné složky vlády, což ovšem znesnadňuje jednotný a koherentní přístup k dané problematice. Pro zajištění bezproblémové spolupráce různých vládních institucí je vhodné pověřit či zřídit vedoucí agenturu či jinou instituci, která je zodpovědná za problematiku kybernetické bezpečnosti a zefektivnění spolupráce mezi vládními aktéry.

2) Spolupráce na mezinárodní úrovni

Mezinárodní spolupráce je výchozím předpokladem pro řešení závažných globálních bezpečnostních témat. Spolupráce na mezinárodní bázi v rámci kyberprostoru vyplývá již ze samotného charakteru internetu. Internet představuje celosvětovou síť spojující počítače a počítačové sítě všech kontinentů. Uživatelé za všech koutů světa jsou schopni mezi sebou komunikovat a vzájemně si vyměňovat data. Vzdálenost v kyberprostoru nehraje žádnou roli. K prosazení svých zájmů na globální scéně je pro stát či nestátního aktéra důležitá kooperace

[39] KLIMBURG, A. (ed.). *National Cyber Security Manual*, 2012: str. 13

[40] Tamtéž: str. 32

[41] Tamtéž: str. 29-34

s širokou škálou mezinárodních partnerů. I na této úrovni se může prosadit hlavní lídr, který bude schopen vést kybernetickou bezpečnostní agendu v rámci systému. Spolupráce probíhá v rámci mezinárodně závazných smluv, politicky závazných dohod, či nevládních dohod mezi certifikačními technickými seskupeními.

3) Spolupráce na národní úrovni

Oblastí kybernetické bezpečnosti se zabývají různé bezpečnostní instituce včetně zpravodajských služeb. Nezbytné je rovněž zapojení privátního sektoru, například subjektů, které se zabývají vývojem nových technologií.

1.6 Pět dilemat kybernetické bezpečnosti[42]

Následující kapitola se zabývá pěti dilematy národní kybernetické bezpečnosti. Ideálním stavem je dosažení rovnováhy mezi ochrannými opatřeními, potřebnými k zajištění bezpečnosti, a případnými náklady vynaloženými na tuto ochranu. Na jedné straně se uvažují výnosy plynoucí z ICT v kontextu ekonomického růstu a osobních svobod a na straně druhé ochrana státu před riziky spojenými s těmito technologiemi.

1.6.1 Rozvoj ekonomiky vs. národní bezpečnost

Rozvoj ekonomiky vs. národní bezpečnost je primárním dilematem, které musí státy zvažovat. Globální ekonomika díky internetu zažívá nebývalý rozkvět. Pro rozvojové země představují informační a komunikační technologie dokonce hnací motor rozvoje. Více než 2,5 miliardy[43] zákazníků nakupuje zboží a služby a provádí elektronické platby přes internet. Mezi služby a aplikace poskytované na internetu patří email, textové zprávy, aplikace umožňující přenos zvuku, videokonference v reálném čase, streamování videí, sociální sítě, elektronické bankovnictví (e-banking), e-learning, mapy, vyhledávače, e-knihy či televize přes internetový protokol IPTV. Ekonomická, sociální, politická a technologická závislost na internetu je natolik vysoká, že jeho ochrana se stala prioritou každého státu.

---

[42] KLIMBURG, A. (ed.). *National Cyber Security Manual*, 2012: str. 34-43

[43] KLIMBURG, A. (ed.). *National Cyber Security Manual*, 2012: str. 3.

Na jedné straně jsou tu výnosy, které ICT a internet přináší, a na straně druhé enormní náklady související ze zajištěním ochrany a bezpečí klíčových systémů a kritické infrastruktury státu.

1.6.2 Modernizace infrastruktury vs. ochrana kritické infrastruktury

Rozvinutá komunikační infrastruktura dosahuje téměř kamkoliv. Průmyslový řídící systém *(Industrial control system - ICS)* představuje základní kámen této kritické infrastruktury, monitoruje procesy a kontroluje příliv informací. Průmyslové řídící systémy jsou obvykle využívané v elektrickém, vodním či ropném a plynovém průmyslu. ICS například zodpovídá za dodávky zemního plynu do elektrárny nebo za přenos elektrického proudu z rozvodné sítě do domácností. Ochrana poskytovatelů veřejných a finančních služeb, telekomunikací a dalších nezbytných služeb spadajících většinou pod privátní sektor je nevyhnutelnou náplní ochrany kritické infrastruktury. V současnosti se většina činností, týkajících se CIP, soustředí na kybernetické aktivity, jako je kybernetický zločin či špionáž. Národní krizový management musí být rovněž rozšířen o kybernetickou složku. Státy si jsou vědomy zranitelnosti těchto systémů, ale vzhledem k povaze útoků, je obrana před nimi velmi složitá. Mezi aktivity, které ohrožují tyto systémy, patří například neautorizovaný přístup, manipulace s daty či jejich úplné zničení.

Neustálý tlak na modernizaci infrastruktury a s tím spojené investice může ohrozit požadavky na zabezpečení těchto zařízení. Dochází ke střetu zájmů, kde na jedné straně jsou vlastnící a řídící pracovníci, jejichž nejdůležitějším cílem je zisk, a na druhé straně vláda, jejímž zájmem je všeobecná ochrana a bezpečí. Východiskem může být nalezení rovnováhy mezi krátkodobými příjmy ze zavedení nových technologií a střednědobými a dlouhodobými ztrátami vycházejícími z nedostatečného zabezpečení. Na druhé straně, pokud systémy a zařízení budou technologicky zaostávat, budou více náchylné k potenciálním hrozbám. Investice do bezpečnostních opatření musí jednak splňovat požadavky vlády, jednak nesmí ohrozit inovace a ekonomický růst.

1.6.3 Veřejný vs. privátní sektor

Mimo úsporná a efektivní opatření je primárním zájmem veřejného sektoru státní bezpečnost. Naopak tomu je v privátním sektoru, kde důležitou roli hraje právě zefektivňování procesů s cílem dosáhnout co nejnižších nákladů a nejvyšších zisků, a obstát tak v konkurenčním prostředí, neboť náklady na záložní systémy a jejich spravování, zcela

převyšují pravděpodobnost a škody možného útoku. Negativní důsledky úspěšně provedeného útoku například v bankovnictví může narušit důvěru klientů v danou banku a vzhledem ke globálnímu charakteru bankovního trhu se tato nedůvěra může šířit i do jiných zemí, kde má daný bankovní ústav pobočky. Riziko, že některý kybernetický útok vyřadí některý ze systému státní kritické infrastruktury, vyplývá z propojení soukromého a státního sektoru při zajišťování bezpečnosti kritické infrastruktury a její závislosti na kybernetickém prostoru. Tyto systémy nespadají pod přímou kontrolu státu a jak již bylo zmíněno výše, soukromé společnosti se snaží vyhnout vysokým nákladům spojeným se správou rezervním systémů. Vysoká závislost státního a soukromého sektoru na kyberprostoru a ICT spolu s nízkou úrovní zabezpečení a ochrany klíčových systémů a kritické infrastruktury státu před potenciálními hrozbami mohou být zneužity teroristy či jinými kybernetickými útočníky.[44]

1.6.4 Ochrana osobních údajů vs. sdílení informací

Další překážku úplného využití přínosů, které s sebou přináší internetová ekonomika, představuje rozpor mezi očekáváním občanů a vládní politikou ochrany osobních údajů a zároveň potřebou sdílení informací za hranicemi států s cílem zvýšit bezpečnost. Obyvatelé států očekávají, že jejich soukromá data zůstanou nedotčena jak ze strany soukromého, tak státního subjektu. Přesto při potírání kriminality, špionáže a dalších ilegálních aktivit v kyberprostoru pomáhá včasná výměna a sledování informací probíhající mezi soukromým a veřejným sektorem. Citlivé údaje často spadají do oblasti působnosti zákonů na ochranu soukromí a ochranu osobních údajů. Zároveň je zde nebezpečí, že informace citlivého obsahu je prozrazena neautorizovanému subjektu nebo je jím odhalena a to může následně vést ke kybernetickým útokům se značným dopadem.[45]

1.6.5 Svoboda projevu vs. politická stabilita

Podle zprávy Rady pro lidská práva je internet nejmocnějším nástrojem 21. století, jehož podstata spočívá v tom, že přispívá k větší transparentnosti přístupu k informacím a

[44] FIŘTOVÁ, M. *Spojené státy v úpadku? Vybrané problémy veřejné politiky v severoamerickém kontextu*, 2013: str. 100-104

[45] KLIMBURG, A. (ed.). *National Cyber Security Manual*, str. 39-40

usnadňuje aktivní zapojení občanů k budování demokratické společnosti.[46] Informační a komunikační technologie tak umožňují širší zapojení občanů do každodenních vládních rozhodovacích procesů. Sociální média jako Facebook, Twitter a další usnadňují sdílení názorů, myšlenek a pocitů a hrála tak například důležitou roli v tuniské a egyptské revoluci, kdy poukázaly na zločiny vládnoucích režimů.[47] Na rozdíl od klasických mediálních kanálů, které přenášejí informace jen jedním směrem a které jsou navíc náchylnější ke státní kontrole kvůli rozsáhlým finančním nákladům, sociální média umožňují vytvářet interaktivní virtuální platformu, kde se může aktivně zapojit každý jednotlivec a diskutovat různá témata, a tím přispívat k pokroku společnosti jako celku. Jedinec nefiguruje jako pasivní příjemce zpráv, ale může se aktivně zapojit do každé diskuze. Zpráva dále odsuzuje snahy států bránit občanům v přístupu k internetu a filtrování jeho obsahu. *„Mělo by být prioritou každého státu zabezpečit přístup k internetu pro všechny své občany.“* [48] Internet se stal klíčovým prostředkem uplatnění práva na svobodu mínění a projevu a jako takový spadá pod článek 19 Všeobecné deklarace lidských práv: „*Každý má právo na svobodu přesvědčení a projevu; toto právo nepřipouští, aby někdo trpěl újmu pro své přesvědčení, a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a bez ohledu na hranice.“*[49]

Snahy autoritářských režimů bránit přístupu svých občanů k internetu jasně demonstruje fakt, že právo svobodné komunikace je silně provázáno s politickou svobodou.[50]

---

[46] UN. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* 2011

[47] ČEJKA, M. *Průvodce inteligentního čtenáře po arabském jaru*, 2012

[48] UN. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* 2011

[49] *Universal Declaration of Human Rights*, 1948

[50] KLIMBURG, A. (ed.). *National Cyber Security Manual*, str. 42

2 Kybernetické hrozby

2.1 Kvalifikace kybernetických hrozeb

Na základě motivu a prostředků útočníka můžeme kybernetické hrozby rozdělit do čtyř hlavních skupin: kyberšpionáž, kyberválka, kyberzločin, a kyberterorismus.[51]

2.1.1 Kybernetická špionáž

Špionáž představuje obor lidské činnosti využívaný k získávání tajných a strategických informací o plánech a aktivitách cizí vlády či konkurenční obchodní společnosti pro účely získání výhody.[52] Kybernetická špionáž se rovněž týká neoprávněného získávání tajných informací. Tallinnský manuál [53] definuje kyberšpionáž takto: *„Jakýkoliv čin prováděný tajně nebo pod falešnou záminkou využívající kybernetické možnosti k získávání informací (nebo pokus o jejich získávání) za účelem poskytnout tyto informace nepřátelské straně konfliktu. Kyberšpionáž musí být prováděna na území kontrolovaném stranou konfliktu.“*[54]

Kybernetickou špionáž lze označit za nejčastější případ aktivit páchaných v kyberprostoru. Je nejčastěji prováděná za účelem odhalení citlivých vládních materiálů, obchodních tajemství či získání informací s cílem zbohatnout či získat moc s minimálními náklady.[55] Obchodní společnosti a vlády neustále čelí případům neoprávněného přístupu do

---

[51] SHACKELFORD, S. *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance,* 2012: str. 1297

[52] Financial Times. *ft.com/lexion*

[53] Tallinnský manuál představuje jakousi příručku týkající se uplatňování práv v kyberprostoru. Vytvořena byla v roce 2009 skupinou nezávislých odborníků z oblasti mezinárodního práva na žádost aliančního centra kyberobrany NATO. Podrobněji vysvětleno v kapitole 2.2.1.

[54] SCHMITT, M. (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013: str. 159

[55] CORNISH, P. *On Cyber Warfare.* 2010: str. 8

jejich informačních technologických systémů a zcizení dat. Pachatelé používají k vniknutí či poškození počítačového systému zákeřný počítačový program malware či se legitimizují jako oprávnění uživatelé.

Státy či nestátní aktéři se uchylují ke kybernetické špionáži za účelem získání ekonomického prospěchu, neboť vyspělé technologie a vědecké poznatky představují hnací motor ekonomického rozvoje. Opakované úspěšné krádeže duševního vlastnictví mohou vést i k oslabení ekonomiky státu. ICT tvoří páteř téměř každé technologie využívané jak pro vojenské, tak civilní účely, a tudíž jsou i hlavním cílem kyberšpionáže.

Existuje velmi tenká hranice mezi kybernetickou špionáží a kyberválkou, neboť je velmi obtížné jednoznačné určit, zda bylo útočníkovým cílem pouze provádět špionáž či útok na daný cíl.[56] Navíc obyčejové mezinárodní právo výslovně nezakazuje ani nijak nereguluje špionáž jako takovou, třebaže jednotlivé státy považují podle svého práva tuto činnost za nelegální.

Kybernetická špionáž pravděpodobně představuje nejsložitější a nejzávažnější hrozbu co se týče svého odhalení. Na základě nepřímých důkazů lze zpravidla zjistit pouze to, že data byla zkopírována. Navíc stopy často ani neodhalí skutečnou identitu útočníka, ale pouze místo odkud se útočník připojil k internetu. To zároveň neznamená, že se jedná o místo odkud byl útok uskutečněn.[57] Nutnost vyvinout takový mechanismus, který by byl schopen reagovat na tyto kybernetické aktivity, vychází ze specifického charakteru kybernetického prostředí. Mezi důležité nástroje při odhalování sofistikovaných kybernetických útoků patří zpravodajské služby a další formy zpravodajských aktivit jako je HUMINT[58], rádiový průzkum, forenzní analýza a v neposlední řadě také spolupráce mezinárodních partnerů při poskytování informací.[59] Důležitý je rovněž mezinárodní dialog s cílem jasně definovat pravidla v kyberprostoru.

---

[56] GOMPERT, David a Martin LIBICKI. Survival. *Cyber Warfare and Sino-American Crisis Instability*. 2014: str. 13

[57] FIŘTOVÁ, M. *Spojené státy v úpadku? Vybrané problémy veřejné politiky*, 2013: str. 96

[58] Kategorie zpravodajství odvozená od informací shromažďovaných a poskytovaných lidskými zdroji.

[59] KLIMBURG, A. (ed.). *National Cyber Security Manual*, 2012: str. 33

2.1.2 Kyberválka

Pro kyberválku neexistuje žádná oficiální či všeobecně akceptovatelná definice, oproti tomu Informační operace ('Information Operations' - Info Ops či IO) či Informační válka (Information Warfare' – IW) jsou běžně používané termíny. Nicméně na akademické půdě je kyberválka běžně diskutovaný termín, který se neodmyslitelně dotýká oblasti mezinárodní bezpečnosti. Předmětem zkoumání je například vznik konfliktů mezi státy v rámci nebo prostřednictvím kybeprostoru a analýza jejich důsledků.[60]

Kyberválka (Cyberwar) je relativně nový fenomén současného, moderního způsobu válčení. A vzhledem k této relativní novosti neexistují žádné mezinárodně zakotvené definice tohoto konceptu. Obecně se jedná o *„útok ze strany nepřátelského státu proti počítačům a sítím jiného státu za účelem způsobení škody nebo narušení systému."*[61]

Clarke a Knake nabízejí státocentrickou definici, kdy kyberválka představuje *„jakékoliv jednání státu za účelem způsobit škodu prostřednictvím infiltrace do počítačů či počítačových sítí jiného státu.*[62] Chatmanhouse zahrnuje do své definice i nestátní aktéry: *„Kyberválka představuje konflikt nejenom mezi státy, ale může zahrnovat i nestátní aktéry. Jakýkoliv protiúder může být kontraproduktivní, neboť cíle můžou být jak vojenské či průmyslové, tak obyčejní civilisté či naopak pouhá „server room", která hostí nespočet klientů, přičemž cíl může být mezi nimi."*[63]

Tallinnský manuál definuje kybernetický útok jako *„kybernetickou operaci defenzivního či ofenzivního charakteru s cílem zranit, usmrtit, poškodit nebo zničit majetek. Za použití síly je považována taková kybernetická operace, která je svou podstatou a následky srovnatelná s operacemi nekybernetického charakteru, které splňují podmínky pro použití síly."*[64]

---

[60] KLIMBURG, A. (ed.). *National Cyber Security Manual*, 2012: str. 17

[61] SHACKELFORD, S. *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance.* 2012: str. 1297

[62] Georgetown Security Studies Review. *Richard A. Clarke and Robert K. Knake's "Cyber War: The Next Threat to National Security and What to Do About It"*, 2010

[63] CORNISH, P. *On Cyber Warfare.* 2010: str. 37

[64] SCHMITT, M. (ed.). *Tallinn Manual on Interneational Law Applicable to Cyber Warfare*, 2012: str. 92 a 47

RAND rozlišuje mezi síťovou a kybernetickou válkou.[65] Zatímco síťová válka se odehrává na společensko-ideové úrovni, kybernetická na úrovni vojenské. Síťová válka (Netwar) je určitý druh války, který je spojen s informacemi a znalostmi společnosti. Může mít podobu propagandy, politické či kulturní podvratné činnosti, infiltrace do počítačových sítí a databází, zviditelnění opozice prostřednictvím internetu. Síťové války jsou charakteristické svým přesahem do politické, ekonomické, sociální, ale i vojenské oblasti. Existuje několik forem síťových válek v závislosti na jejich aktérech:

1) Síťové války mezi státy;
2) mezi státem a nestátním aktérem;
3) mezi nestátními aktéry navzájem.

Nejcharakterističtější znaky kyberválky podle Arquuilly[66] a Cornishe[67] jsou:

- Aktéři kyberválky mohou dosáhnout svých politických či strategických cílů bez použití násilí v ozbrojeném konfliktu;
- následkem kyberválky dochází k redistribuci moci mezi relativně slabší a jinak bezvýznamné aktéry, moc uplatňují nejenom státy, ale i nestátní aktéři;
- falešné IP adresy, zahraniční servery či internetové přezdívky poskytují aktérům anonymitu při páchání svých trestných činů;
- hranice vojenské versus civilní, fyzické versus virtuální se v kyberprostoru stírají;
- asymetrické nepřátelské útoky;
- není nutně závislá na vyspělých technologiích – organizační a psychologická složka hraje stejně důležitou roli jako složka technická;
- výsledky kyberválky jsou obvykle krátkého trvání, když potenciální oběť zjistí, že jeho síť byla napadena, napadené systémy mohou být během několika hodin či dní opraveny, obnoveny či nahrazeny;
- nesnadnost opakování kyberútoků - kybernetické útoky využívají slabá místa v napadeným sítích – napadený je motivován své obranné prostředky neustále zlepšovat a útočník má tak menší pravděpodobnost, že jeho příští útok bude stejně účinný;

---

[65] ARQUUILLA, J. *Cyberwar is coming!,* 1993: str. 27-32

[66] Tamtéž: str. 8

[67] CORNISH, P. *On Cyber Warfare.* 2010: str. 7

- nejednoznačnost výsledků a nesnadnost vyhodnocení záměrů – jakákoliv kybernetická operace může vést k domněnce, že bude doprovázena konvenční válkou bez ohledu na to, zda-li to bylo útočníkovým cílem;
- nesnadnost rozeznání, zda se jedná o kybernetický útok doprovázený konvenční válkou nebo o pouhou kybernetickou špionáž – kybernetická špionáž může být interpretována jako předzvěst války;
- špatně provedený kybernetický útok může projít bez povšimnutí, může být zastaven firewallem, aniž by si toho někdo všiml;
- provádění kybernetických útoků je mnohem jednodušší než konvenční vedení války a může být prováděn mimo státní autority.

Vojenství v informačním věku využívá bezpočet technologických vynálezů k zajištění ochrany státu. Bomby jsou naváděné pomocí GPS satelitů, rychlým tempem roste význam bezpilotních letounů, a i voják v terénu je vybaven pomocnou elektronikou. Přílišná závislost vojenských sil na informačních a komunikačních technologiích v současném digitálním světě však přináší kromě užitku i prostor pro zneužití. Kyberprostor je otevřené prostředí, kde si žádný stát nemůže nárokovat dominantní postavení.

Mezi případy kybernetických útoků patří například politicky motivovaný útok na Estonsko v roce 2007 skupinou hacktivistů.

Tato událost byla nejdříve považována za kybernetickou válku, ale později se však od tohoto názoru opustilo. DDoS[68] útoky přehltily a vyřadily tak z provozu vládní stránky, weby politických stran, médií a bank. Vzhledem k tomu, že nedošlo k žádnému fyzickému poškození systémů, mezinárodní společenství se shodlo na tom, že se nejedná o formu ozbrojeného útoku. [69] Rozhodující událostí v tomto směru byl kybernetický útok prostřednictvím počítačového červa Stuxnet, na jehož vývoji se podíleli odborníci z Izraele a USA.[70] Cílem viru byla oblast íránských průmyslových řídících systémů pro obohacování uranu. Stuxnet fyzicky zničil centrifugy, a tudíž se jedná o kybernetickou operaci splňující

[68] DDoS – Distributed Denial of Service představuje techniku útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.

[69] SCHMITT M. (ed.). *Tallinn Manual on Interneational Law Applicable to Cyber Warfare*, 2012: str. 56

[70] SANGER, D. *Obama Order Sped Up Wave of Cyberattacks Against Iran*, 2012

podmínky ozbrojeného útoku.[71] Navíc byl útok proveden velmi sofistikovaně a odborníci se shodli na tom, že musel být proveden za podpory státu. Již od počátku byly podezřívány právě Spojené státy a Izrael.

Kybernetická válka je charakteristická nejednoznačnými výsledky a efektivností. Útoky využívají moment překvapení a z počátku bývají masivnější. Napadený se okamžitě snaží vyhledat citlivá místa ve své obraně a zintenzivní zabezpečení svých systémů. Příkladem je Irán, který je po útoku Stuxnetu mnohem opatrnější a ostražitější k tomu, jaká zařízení jsou připojena k sítím, které kontrolují centrifugy na obohacování uranu. A mnohem ostražitější k odchylkám mezi tím, jak jeho centrifugy mají pracovat a jak doopravdy pracují. Z této logiky vyplývá, že další útoky budou muset být odlišné, komplexnější a možná budou i méně úspěšné než ty původní, využívající moment překvapení. Naopak neúspěšný útok může projít bez povšimnutí anebo útoku není připisována náležitá závažnost, která by si vyžadovala odvetný úder. I když kybernetický útok nemusí být nutně destabilizujícím činitelem, může bezprostředně zahájit vojenský konflikt. A to v situaci, kdy napadený nemá dostatek času k vyhodnocení situace (rozhoduje se pod tlakem). Výsledkem může být zbytečná eskalace konfliktu, kdy je kybernetický útok považován za předzvěst války. Nebezpečí, že kybernetický útok povede k ozbrojenému konfliktu tkví v nejednoznačnosti či špatné interpretaci jeho dopadů.[72]

2.1.3 Kyberzločin

„Kyberprostor je stále ještě ideálním prostředím pro organizovaný zločin s vidinou velkého zisku a malého rizika.“[73] Kyberzločinem se rozumí *„široká škála různých druhů trestné činnosti, páchané online, jejichž primárním nástrojem nebo cílem jsou počítače a informační systémy. Pro tyto trestné činnosti je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení,*

[71] SCHMITT M. (ed.). *Tallinn Manual on Interneational Law Applicable to Cyber Warfare*, 2012: str. 59

[72] GOMPERT, David a Martin LIBICKI. Survival. *Cyber Warfare and Sino-American Crisis Instability*. 2014: str. 14-15

[73] CARR Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*, 2009

nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.“[74] Trestné činnosti páchané v kyberprostoru se mohou dotýkat přímo jednotlivců, jako je například krádež identity, nabourání se do emailových účtů či obchodních společností, kde se jedná například o krádež duševního vlastnictví firmy nebo států, kde by rozsáhlý kybernetický trestný čin cílený na narušení kritické infrastruktury mohl vážně ohrozit národní bezpečnost.

Kyberzločin může být rozdělen do třech oblastí[75]:

1) Tresné činy specifické pro počítače a informační systémy – jedná se o útoky proti informačním systémům a tzv. phishing[76] specifické pro internet. Patří sem například nabourání se do bankovních účtů a přesměrování plateb přes falešné webové stránky banky, krádeže osobních údajů a podobně.

2) *Tradiční trestné činy* – jde například o podvody spojené s nedodáním objednaného zboží, padělání a krádež identity. Tradiční trestné činy jsou páchány prostřednictvím nástrojů, jako je například phishing, spam a malware.

3) *Trestné činy související s nelegálním a škodlivým obsahem* - online šíření dětské pornografie, podněcování k rasové nenávisti, šíření teroristických návodů a podněcování k teroristickým útokům a oslavování násilí, terorismu, rasismu a xenofobie.

2.1.4 Kyberterorismus

Často diskutovaným jevem v současném „kyber“ světě je rovněž kyberterorismus. Přesné vymezení tohoto fenoménu v rámci mezinárodní diskuze však zatím neexistuje.

---

[74] Ministerstvo vnitra České republiky, *Základní definice, vztahující se k tématu kybernetické bezpecnosti*, 2009

[75] European Comission. *What is cybercrime?*, 2015

[76] Podstatou phishingu je zcizování digitální identiy uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich následného zneužití jako například výběr hotovosti z konta, neoprávněný přístup k datům. Phising má většinou formu klasické emailové zprávy a imituje důvěryhodného odesílatele, aby tak zamaskovala svůj podvodný záměr, jímž je vylákat údaje od uživatele.

Obecně terorismus představuje násilnou formu prosazování politických zájmů stoupenců určité radikální ideologie (politické, náboženské, nacionalistické, separatistické, ekologické a jiné). Cílem může být ovládnutí určitého území. Častými obětmi bývají nevinní civilisté.[77] Naopak kyberterorismus operuje skrze kyberprostor a využívá jej k tomu, aby *„narušil počítačové nebo telekomunikační služby a následkem rozsáhlého narušení systému by došlo ke ztrátě důvěry veřejnosti ve funkčnost vlády"*.[78]

Nejvíce citovanou prací, týkající se tématu kyberterorismu, je *Testimony before the Special Oversight Panel on Terrorism* od Dorothy E. Denningové z roku 2000. Denningová definuje kyberprostor následovně:

„*Kyberterorismus je konvergencí terorismu a kyberprostoru. Je obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným za účelem zastrašit nebo donutit vládu nebo občany k podporování sociálních nebo politických cílů. Kybernetickým útok je násilný útok proti osobám nebo majetku, při nejmenším takový útok musí vyvolat strach. Příkladem jsou takové útoky, které vedou ke smrti nebo k tělesným zraněním. Mají podobu explozí, havárie letadla, kontaminace vody, či kritické poškození ekonomiky. Závažné útoky proti kritické infrastruktuře jsou považovány za akt kyberterorismu. "*[79]

Z definice Denningové vyplývá, že přítomnost násilí je zásadní podmínkou pro kvalifikaci kyberterorismu. Co se týče mezinárodní bezpečnosti, doposud nebyl zaznamenán žádný kybernetický čin, který by považován za kybernetický teroristický útok. Současné kybernetické útoky jsou schopné způsobit rozsáhlou ekonomickou škodu nebo nepřímo vést k i k fyzickému násilí, ale způsobit skutečné násilí ve smyslu přivodit smrt jako například bombový útok, je velmi nepravděpodobné. Existují sice snahy o narušení masové komunikace jako například útoky skupiny hackerů zvané Anonymous, ale zatím můžeme považovat kybernetický terorismus za téma budoucnosti. Reálnou hrozbou však zůstává využívání internetu teroristickými skupinami pro různé účely: ke komunikaci, rekrutování, financování, šíření propagandy a organizování svých aktivit.

---

[77] Bezpečnostní informační služba. *Terorismus*

[78] SHACKELFORD, S. *Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance,* 2012: str. 1301

[79] DENNING, D. *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 2000

Kontroverzním tématem však zůstává rozlišení mezi kybernetickou špionáží na jedné straně a kyberzločinem a vojenskými kybernetickými aktivitami na straně druhé. Je totiž velmi obtížné se vůbec dopátrat, zda je pachatelem stát či kriminální skupina jednající v jeho zastoupení, či pachatel jedná sám za sebe.[80]

2.2 Mezinárodní spolupráce v oblasti kyberprostoru

Alianční centrum kyberobrany NATO (The NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE) je mezinárodní vojenská organizace sídlící ve městě Tallinn v Estonsku, která vznikla v roce 2008 z popudu Severoatlantické rady. Centrum nespadá pod velení ani vojenské složky NATO a ani jím není sponzorováno, nicméně je součástí širší struktury podporující NATO Command Arrangements. Organizace je financovaná a řízena mezinárodním řídícím výborem sestávajícím z představitelů přispívajících států, mezi něž patří Česká Republika, Estonsko, Francie, Německo, Maďarsko, Itálie, Litva, Lotyšsko, Nizozemí, Polsko, Slovensko, Španělsko, Velká Británie a Spojené státy americké. Austrálie se rovněž podílí jako aktivní přispěvatel. Mezi základní cíle organizace patří zvýšení spolupráce, schopností a výměny informací mezi NATO, členskými státy a partnerskými státy v oblasti kybernetické obrany prostřednictvím výzkumu, vzdělávání a konzultací.[81] Organizace si osvojila interdisciplinární přístup pro uskutečňování svých aktivit a to zejména vědecký výzkum týkající se kybernetické oblasti z právního, strategického, technického a dalšího hlediska. Mezi jiné prostředky patří také poskytování vzdělávání a školení, pořádání konferencí a workshopů či různá praktická cvičení týkající kybernetické bezpečnosti a konzultace.

2.2.1 Tallinnský manuál

V roce 2009 přizvalo Centrum skupinu nezávislých odborníků z oblasti mezinárodního práva, aby vytvořila příručku týkající se uplatňování práv v kyberprostoru. Jejím úkolem bylo aplikovat existující právní normy na tuto novou formu válčení. Výsledkem tohoto procesu byl právně nezávazný dokument *Tallinn Manual on the International Law*

[80] KLIMBURG, A. (ed.) *National Cyber Security Manual*, 2012: str. 32

[81] Tamtéž.

Applicable to Cyberwarfare nebo zkráceně Tallinn Manual vydaný v roce 2013 Cambridge University Press, který následuje Tallinn 2.0 a dále pak kurz International Law of Cyber Operations, který vychází z obou předchozích dokumentů a nabízí zájemcům podrobný přehled o aplikaci mezinárodního práva v kyberprostoru.

Tallinnský manuál se věnuje zejména problematice „ius ad bellum“[82] a „ius in bello[83]“ a v rámci těchto témat se zaobírá i otázkou státní suverenity, odpovědnosti či mořského práva. Soustředí se zejména na nejvážnější a zároveň nejničivější formy kybernetických operací, které jsou kvalifikovány jako ozbrojené útoky a tudíž na ně státy mohou reagovat v sebeobraně, jako by se jednalo o ozbrojený konflikt. Nutno poukázat na to, že dokument není oficiálním vyjádřením stanoviska NATO, Centra či jeho členů a ani neodráží vojenskou doktrínu Severoatlantické aliance, nýbrž se jedná o nezávislý názor skupiny odborníků vycházející z jejich znalostí a praxe.[84]

Tallinn 2.0 rozšiřuje předchozí verzi Tallinnského manuálu o kybernetické operace menšího rozsahu, které nesplňují podmínky ozbrojeného konfliktu, ale přesto mohou způsobit státům nemalou škodu. Předpokládaným termínem publikování dokumentu Tallinn 2.0 je rok 2016.

2.2.2 Úmluva o kyberzločinu

V roce 1997 Rada Evropy ustavila Komisi expertů na zločin v kyberprostoru. Výsledkem jejího snažení byla Úmluva o kyberzločinu (Convention on Cybercrime, ETS 185), otevřená k přístupu dne 9. února 2005, a to i pro nečlenské země. Úmluvu podepsalo 50 států. Úmluva představuje první mezinárodněprávní nástroj určený k řešení problémů v oblasti počítačového zločinu s mezinárodním přesahem. Její signatáři jsou povinni kriminalizovat určitá jednání, která svým charakterem spadají do oblasti počítačového zločinu, a zároveň jsou signatářské země povinné přijmout procesní normy umožňující takovou trestnou činnost postihovat. Úmluva rovněž uvádí konkrétní principy a metody vzájemné spolupráce a pomoci mezi jednotlivými státy při vyšetřování informační kriminality, včetně způsobů předávání zajištěných dat, vydávání osob a jinou podporu, která

[82] Právnický pojem označující právo státu zahájit válku.

[83] Právnický pojem označující pravidla vedení války.

[84] NATO Cooperative Cyber Defence Centre of Excellence. *Tallin Manual Process* [online]. 2015 [cit. 25.4.2015]. Dostupné z: https://ccdcoe.org/tallinn-manual.html

by státům usnadňovala vzájemnou spolupráci.[85] Nicméně signatářské státy mají možnost odmítnout spolupráci, pokud se domnívají, že by to mohlo ohrozit jejich suverenitu, bezpečnost, veřejný pořádek či jiné zájmy.[86] Navíc Úmluva nestanovila žádný donucovací mechanismus, který by ukládal státům, aby plnily své závazky.

2.2.3 Deset pravidel kybernetické bezpečnosti

Článek *Ten Rules for Cyber Security*[87] od Enekena Tikka vydaný v roce 2011 se snaží rozvinout debatu ohledně pravidel v kybernetickém prostoru. Zaměřuje se spíše na již existující právní koncepty, než na vytváření úplně nového právního přístupu. Zároveň však poukazuje na potřebu lepších zákonů upravujících například ochranu dat nebo povinnosti poskytovatelů internetového připojení, které by odpovídajícím způsobem reagovaly na současné hrozby.[88] Deset pravidel se zaměřuje zejména na chování států v kyberprostoru. E. Tikk tvrdí, že pokud by kybernetický útok splňoval podmínky ozbrojeného útoku, bylo by přípustné se proti takovému útoku bránit podle článku 5 Severoatlantické smlouvy[89]: *„Smluvní strany se dohodly, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem, a proto odsouhlasily, že dojde-li k takovému ozbrojenému útoku, každá z nich uplatní právo na individuální nebo kolektivní sebeobranu, uznané článkem 51 Charty Spojených národů, pomůže smluvní straně nebo stranám takto napadeným tím, že neprodleně podnikne sama a v souladu s ostatními stranami takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a udržet bezpečnost severoatlantické oblasti.“*[90]

Deset pravidel kybernetické bezpečnosti je uvedeno v následující tabulce:[91]

---

[85] Mezinárodní spolupráce v boji proti informační kriminalitě.

[86] Council of Europe. *Convention on Cybercrime*, 2001

[87] TIKK, E. *Ten Rules for Cyber Security*, 2011

[88] Tamtéž: str. 120-121

[89] Tamtéž: str. 124

[90] *The North Atlantic Treaty*, 1949

[91] DOLEŽEL, M. *NATO svazuje kyber-prostor,* 2001

Tabulka 2 – Deset pravidel kybernetické bezpečnosti

1.	Pravidlo teritoriality	Informační infrastruktura nacházející se na území jednoho státu je předmětem teritoriální suverenity onoho státu.
2.	Pravidlo odpovědnosti	Spáchání kyberútoku z počítačů a jiných zařízení nacházejících se na území jednoho státu je považováno za důkaz a tento útok může být tomuto státu připisován.
3.	Pravidlo spolupráce	Pokud byl útok spáchán z počítačových systémů daného státu, je tento stát povinen spolupracovat s obětí formou konzultací, výměny informací, a dalšími způsoby.
4.	Pravidlo sebeobrany	Každý má v kyberprostoru právo na sebeobranu. Reakce silou je za některých okolností přípustná.
5.	Pravidlo ochrany dat	Data získaná monitorováním internetu jsou považována za osobní. Mohou však být poskytnuta třetí straně, pokud zajistí stejnou míru ochrany. Monitorování internetu a výměna informací musí být v rovnováze s ochranou práv jedince.
6.	Pravidlo odpovědnosti se starat	Každý má odpovědnost snažit se rozumným způsobem ochránit svá počítačová zařízení.
7.	Pravidlo včasného varování	Každý má povinnost informovat potenciální oběť o chystaném kyberútoku.
8.	Pravidlo přístupu k informacím	Veřejnost má právo být informována o kyber-hrozbách vůči životu, bezpečnosti a dobrému žití.
9.	Pravidlo zákonnosti	Každý stát je povinen zahrnout nejčastější kyber-zločiny do svého právního řádu.
10.	Pravidlo mandátu	Schopnost organizace jednat vždy vychází z rozsahu jejího mandátu. Na mezinárodním poli je nutné zastavit duplikaci schopností a úsilí.

Zdroj: DOLEŽEL, M. ***NATO svazuje kyber-prostor,*** **2001**

3 Spojené státy americké a kyberprostor

Spojené státy americké považují kritickou informační infrastrukturu za páteř prosperující ekonomiky, silné armády, transparentní vlády a svobodné společnosti. Ochrana kyberprostoru se stala základní prioritou americké vlády a kybernetické bezpečnosti je věnováno mnoho vládních dokumentů. Mezi významné dokumenty patří například Mezinárodní strategie pro kyberprostor (2011)[92], Strategie ministerstva obrany (2011)[93] nebo nejnovější Národní strategie pro výměnu a ochranu informací (2012).[94] Zajištění bezpečného kyberprostoru je rovněž zakotveno v Národní bezpečnostní strategii Spojených států (2010)[95]. *„Kybernetické hrozby představují jednu z nejnebezpečnějších výzev pro náš národ, které ohrožují národní a veřejnou bezpečnost a ekonomiku státu.“*[96] Vedle moře, vzduchu, země a vesmíru považují Spojené státy kyberprostor za pátou doménu, kde je možné, pokud to bude nevyhnutelné, použít vojenskou sílu.[97] Podle strategie ministerstva obrany je *„považování kyberprostoru za doménu důležitým předpokladem pro aktivity podporující národní bezpečnostní zájmy.“* [98] V neposlední řadě Spojené státy kladou důraz na zachování otevřeného, bezpečného a spolehlivého internetu. Největší prioritou kybernetické bezpečnosti je ochrana kritické infrastruktury a informačních systémů před kybernetickými hrozbami.

Kybernetické bezpečnosti se v rámci Spojených států amerických věnuje několik vládních agentur. Mezi nejdůležitější subjekty, aktivní v této oblasti, patří:[99]

---

[92] The White House. *International Strategy for Cyberspace*, 2011

[93] Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, 2011

[94] The White House. *National Strategy for Information Sharing and Safeguarding*, 2012

[95] The White House. *National Security Stratety*, 2010

[96] Tamtéž: str. 27

[97] Tamtéž: str. 22

[98] Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, 2011: str. 5

[99] FIŘTOVÁ, M. *Spojené státy v úpadku? Vybrané problémy veřejné politiky*, 2013: str. 91-92

1) Armádní kybernetické velitelství (United States Cyber Command, CYBERCOM) představuje nejvyšší velení kybernetických jednotek a je začleněno v rámci Strategického velení (Strategic Command, STRATCOM) Ministerstva obrany USA. Zahrnuje jednotky námořnictva, pozemních a leteckých sil.

2) Centrum kybernetické kriminality při Ministerstvu obrany (Department of Defence Cyber Crime Center, DoD CCC, DC3)

3) Národní bezpečnostní agentura (National Security Agency, NSA), Federální úřad pro vyšetřování (Federal Bureau of Investigation, FBI) a Ústřední zpravodajská služba (Central Intelligence Agency, CIA). Jejich role spočívá hlavně ve shromažďování informací, nikoli v účasti na kybernetických operací.

4) Ministerstvo vnitřní bezpečnosti (Department of Homeland Security) má za úkol chránit sítě a systémy federální vlády.

Priority v oblasti kybernetické bezpečnosti:[100]

1) Ochrana kritické infrastruktury a informačních systémů před kybernetickými hrozbami;
2) zdokonalování se v odhalování a informování o útocích, aby na ně bylo možné co nejrychleji reagovat;
3) spolupráce s mezinárodními partnery vedoucí k podpoře svobody internetu a položení základů otevřeného, bezpečného a spolehlivého kyberprostoru;
4) určení si jasně definovatelných bezpečnostních cílů a zajištění, aby tyto cíle byly zodpovědně naplňovány;
5) vytváření pracovní síly znalé v oboru a spolupráce s privátním sektorem.

[100] The White House. *Foreign Policy – Cybersecurity* [online]. 2015 [cit. 25.4.2015]. Dostupné z: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

4 Čínská lidová republika a kyberprostor

Obsahem následující kapitoly bude analýza přístupu ČLR ke kybernetickému prostoru. Čínská civilní kybernetická strategie je ztělesněna v tzv. *Dokumentu 27: Prohlášení o posílení informační bezpečnosti z roku 2003*[101] a po něm následuje *Doporučení na podporu rozvoje informačních technologií a informační bezpečnosti*[102] uveřejněné v roce 2012. Obě strategie zdůrazňují kontrolu a monitorování internetu, rozvoj kritické infrastruktury, podporu vedení a řízení informační bezpečnosti, podporu rozvoje ve všech oblastech. Doporučení z roku 2012 navíc poprvé uvažuje rozvoj informačních technologií ve spojitosti se zlepšením života a sociálních a ekonomických podmínek občanů.[103]

4.1 Čínské vnímání hrozeb v kyberprostoru

Čínská národní strategie *The Scientific Outlook on Development* obsahuje závazek vlády k budování státní moci pod kontrolou Čínské komunistické strany a k ochraně klíčových zájmů týkajících se národní suverenity, bezpečnosti, územní celistvosti a mírového rozvoje. Klíčovým okruhem zájmu národní strategie je rovněž vývoj v oblasti kyberprostoru, jakožto předpokladu ekonomického, polického a vojenského pokroku a nástroje k získání informační dominance v domácím a mezinárodním prostředí. Čína rozděluje kybernetické

[101] CPC Central Committee and State Council. *Opinions for Strengthening Information Security Assurance Work*, 2003

[102] The Central People`s Government of the People`s Republic of China. *State Council Opinion on Vigorously Promoting the Development of Informatization and Effective Protection of Information Security*, 2012

[103] CHANG, A. *Warring State: China`s Cybersecurity Strategy*, 2014

hrozby do tří oblastí: hacking[104] a kyberzločin, internetový informační management a propaganda a v neposlední řadě vojenská zranitelnost.[105]

Čínská média prohlašují, že co se týče kybernetických útoků, jejichž většina pochází ze zahraničí, je *„Čína obětí číslo jedna“.*[106] Otázky hackingu a kyberzločinu by měly spadat do oblasti vnitrostátního a mezinárodní práva. Ostatní kybernetické útoky, jako například bankovní podvody, hazard a další kyberzločiny, jsou páchány na domácí půdě. Kontrola internetu a jeho management se jeví jako zásadní ochranné opatření před destabilizací čínského politického systému, neboť čelní představitelé vnímají sociální sítě, jako je Facebook, Twitter, Instagram a další, kde dochází k přístupu a výměně informací mezi uživateli, jako zdroj *„dezinformace, fám, chaosu, politické destabilizace a teroru, který může způsobit paniku a vést k sociální krizi a svrhnout režim“.*[107] Zdrojem hrozeb jsou opět jak zahraniční, tak vnitrostátní aktéři. Pojem vojenská zranitelnost odráží uvědomění si rizika využití informační technologie a systémů pro vojenské účely a zároveň vnímání americké dominance v kyberprostoru jako největšího zdroje zranitelnosti pro čínské bezpečnostní a vojenské systémy.[108]

4.2 Čínská internetová cenzura

Primárním cílem čínské vlády je zajištění informační bezpečnosti, a to včetně otevřené cenzury. Čína disponuje nejdůmyslnějším režimem kontroly internetu a toků informací na světě. Zatímco dochází k neustálému nárůstu internetových uživatelů, čínské vládní orgány a soukromé firmy současně vyvíjejí nástroje a způsoby, jak omezit či upravit obsah, tak aby posiloval legitimitu režimu, včetně známého „great firewall of China“. Great firewall je navržen tak, aby prostřednictvím automatického přesměrování, filtrování domén, URL a

[104] Pojem Hacker se často nesprávně používá pro osoby, které zneužívají svých znalostí při pronikání do informačního systému a tak porušují zákon.

[105] Institute on Global Conflict and Cooperation. *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, 2012: str. 8

[106] Tamtéž: str. 8

[107] Tamtéž: str. 8

[108] Tamtéž: str. 9

dalších nástrojů, oddělil čínský kyberprostor od zbytku světa.[109] Čínská vláda zastává myšlenku internetové suverenity, kdy každá země má právo kontrolovat svůj internetový prostor. Tento přístup sdílí také blok afrických a arabských zemí, spolu se SNS v čele s Ruskou federací. USA, Evropská unie a další západní země nesouhlasí s vysokou mírou kontroly internetu, neboť zastávají svobodný a otevřený internet se zapojením soukromého sektoru a občanské společnosti při řízení internetu.[110] Cenzura by v západních zemích nebyla možná, neboť lidé považují internet za prostor, kde se mohou svobodně vyjádřit, a tudíž by jakákoliv restrikce internetu byla vnímána jako narušení tohoto práva. Čína odmítá západní pohled na řízení internetu bez kontroly a poukazuje na kulturní odlišnosti v kyberprostoru: *„kulturní odlišnosti a tradice mezi státy jsou zásadní příčinou rozdílných národních kybernetických strategií, a proto bychom měli přikládat větší význam kulturním prvkům, z kterých vychází politika řízení internetu v odlišných zemích.“*[111]

Koncept internetové suverenity byl uveřejněn již v roce 2010 v oficiální vládní zprávě *The Internet in China*[112]: *„Předpokládá se, že všechny osoby a organizace působící na čínském území budou dodržovat všechny zákony a předpisy týkající se internetu, neboť internet na čínském území podléhá jurisdikci čínské suverenity.“*[113]

Vláda zaměstnává statisíce lidí, kteří vstupují na diskuzní fóra a blogy a usměrňují debaty svými komentáři vlasteneckého charakteru.[114] Vláda nejen blokuje obsah na webových stránkách, ale také dohlíží nad uživateli internetu a kontroluje, za jakým účelem internet využívají. Amnesty Interneational dodává, že Čína *„má největší zaznamenaný počet uvězněných novinářů a „kyber“ disidentů na světě“*.[115] Díky pevné kontrole předních médií může vláda snadno manipulovat s veřejným míněním a v kombinaci s rozsáhlým aparátem kontroly internetu může zcela potlačit domácí diskuze týkající se témat, jako je oblast lidských práv, disentu, nezávislost Tibetu nebo otázka Taiwanu.[116]

---

[109] YU, M. *Party Directs China`s Twitter*, 2012

[110] FEAKIN, T. *ARF, and how to change the tune of the cyber debate, 2013*

[111] Tamtéž.

[112] China Daily.com.cn. *White paper on the Internet in China*, 2010

[113] TIEZZI, S. *China's 'Sovereign Internet'*, 2014

[114] MACKINNON, R a MOROZOV, E. *Firewalls to Freedom*, 2009

[115] YU, M. *Party Directs China`s Twitter*, 2012

[116] Council on Foreign Relations. *U.S. Internet Providers and the 'Great Firewall of China'*, 2011

4.3 Koncept informatizace a kyberválka

Cílem procesu informatizace vyhlášeného v dokumentu *„The State Informatization Development Strategy (2006-2020)“* je urychlení transformace průmyslové společnosti ve společnost informační. Mezi klíčové aspekty informatizace v nadcházejících 15 letech patří například podpora integrace informačních a komunikačních technologií v oblasti národní ekonomiky, společenského života, budování vyspělé internetové kultury a zajištění bezpečnosti informačních systémů.

Myšlenka budování informačních schopností PLA se objevila počátkem 90. let minulého století jako reakce na vojenské postavení Spojených států amerických. Demonstrace americké vojenské síly a rozhodující role informačních technologií ve válce v Perském zálivu (1991) přesvědčila mnoho států, že přímá konfrontace s USA by vedla k ničivé porážce. Teoretikové v rámci PLA usoudili, že zdroj americké vojenské síly tkví v RMA. Informační válka byla chápána jako nástroj v boji proti americké moci a zároveň způsob, jak získat asymetrickou výhodu proti mnohem silnějšímu protivníkovi.[117] PLA vychází z velké části z amerického konceptu network-centric warfare (NCW), kde je hlavní důraz kladen na rozvoj systému C4IRS.[118] Čínští stratégové používají stejnou terminologii jako americké ozbrojené síly: CNO (computer network operations), CNA (computer network attack), CND (computer network defense), CNE (computer network exploitation).[119] PLA chápe kybernetickou válku jako součást moderního válčení v informačním věku. Čínské zdroje definují kyberválku jako „*využití síťových technologií a metod v boji s nepřátelskou stranou za účelem získání informační výhody v politické, ekonomické, vojenské a technologické oblasti.“* [120] Kybernetické operace mají penetrovat, využít, popřípadě poškodit nebo sabotovat prostřednictvím elektronických nástrojů informační systémy a sítě, počítače a komunikační

[117] WORTZEL, L. *The Chinese People`s Liberation Army and Information Warfare*, 2014: str. 1-3

[118] Efektivní systém velení na bázi C4ISR neboli velení, řízení, spojení, výpočetní technika, informatizace, vojenské zpravodajství, sledování a průzkum je podmínkou účinného plánování, přípravy, organizace a řízení ozbrojených sil a efektivního velení. Je to moderní, pružný systém, založený a využívající nejnovější technologie.

[119] CARR Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*, str. 173

[120] KRAMER, F. *Cyberpower and National Security*, 2009: str. 466

systémy i podpůrnou infrastrukturu nepřítele. Jsou mimo jiné úzce spojené s aktivitami ve vesmíru, tradičními formami špionáže a shromažďováním informací. Koncept kyberválky vychází z tradičního strategického čínského myšlení.[121]

Informatizace se stala zásadním předpokladem pro modernizaci čínské armády. Aktivní obrana ČLR znamená, že PLA je zcela připravená vyhrát lokální války v podmínkách informatizace neboli za použití vyspělých počítačových systémů, informační technologie a komunikačních sítí. A zároveň vylepší a rozvine strategický koncept „people`s war"[122]; čínská vláda tak může získávat technické odborné znalosti od civilního obyvatelstva, a vytvářet tak civilní kybernetickou milici.[123] Americké ministerstvo obrany ve své roční zprávě kongresu *Military and Security Developments Involving the People's Republic of China 2012* poznamenává, že pojem „lokální válka" může být rovněž přeložen jako „regionální válka". Vedou se spory o to, který termín je přesnější.[124]

ČLR si uvědomuje roli kybernetické války a důležitost informace v současném informačním věku a je velmi aktivní v rozvíjení své vojenské strategie a doktríny pro vedení informačních vojenských operací, jejichž cílem je získání informační dominance nad protivníkem. A zároveň si uvědomuje zranitelnost USA, jíž je vysoká míra závislosti na informačních a komunikačních technologiích.

Podle dostupných zdrojů se čínská kybernetická doktrína zabývá zejména kontrolou internetu a informací za účelem zachování politické stability. Pro ČLR je rovněž důležitý proces informatizace s cílem budování silné ekonomiky a rozvoj vyspělých technologií určených k zneškodnění vojenských systémů kontroly a řízení a zbraňových systémů protivníka. Použití kybernetických zbraní ke zneškodnění infrastruktury protivníka však nepatří mezi hlavní priority.[125]

---

[121] WORTZEL, L. *The Chinese People`s Liberation Army and Information Warfare*, 2014: str. 16

[122] College of Defence Studies, NDU, PLA, CHINA. *National Defense Policy*

[123] CARR Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*, str. 172

[124] Annual Report to Congress. *Military and Security Developments Involving the People's Republic of China 2012,* 2012: str. 3

[125] LEWIS, A. a HANSEN, S. *China's cyberpower: International and domestic priorities*, 2014: str. 2

5 Čínsko-americká spolupráce v rámci kybernetické bezpečnosti

Obě vlády se shodují na tom, že je nutné v rámci mezinárodního společenství prosazovat bezpečný, otevřený a mírumilovný kyberprostor. Jsou ovšem oblasti jako je například míra kontroly internetu a suverenita v kyberprostoru, kde mají země zcela odlišné zájmy.

5.1 Centrální témata kyberprostoru z čínského a amerického pohledu

Čínské oficiální stanovisko vládních, akademických a vojenských kruhů k problematice kyberprostoru se týká následujících témat: digitální propast, militarizace kyberprostoru a rozšíření státní suverenity na oblast kyberprostoru.[126]

Čína upozorňuje na tzv. digitální propast mezi rozvinutými a rozvojovými zeměmi. Digitální propast vyjadřuje *„ekonomickou a sociální nerovnost mezi skupinami osob v dané populaci, která úzce souvisí s přístupem, užitím a znalostí informačních a komunikačních technologií (ICT)*“[127]. ČLR sama sebe považuje za rozvojovou zemi. Zároveň ČLR je toho názoru, že USA zneužívají svou pozici lídra v oblasti globálních informačních technologií a tzv. „Internet governance“ k sestavení takových mezinárodních norem, které by upravovaly kyberprostor ve prospěch USA.

Čína veřejně prohlašuje, že její kybernetické vojenské schopnosti mají pouze defenzivní charakter a disponuje jimi pro svou vlastní ochranu před případným útokem ze strany USA. Podle čínských zdrojů hegemonické snahy a útočné schopnosti Spojených států v kyberprostoru vedou k militarizaci kyberprostoru. Tato tvrzení opírají o výklad v americké mezinárodní strategii pro kyberprostor (*International Strategy for Cyberspace): “Spojené*

[126] HSU, K. *China and International Law in Cyberspace*, 2014: str. 1-2

[127] OECD. *Glossary of Statistical Terms – Digital divide*, 2002

státy americké odpoví na jakýkoliv nepřátelský akt pocházející z kyberprostoru, tak jako bychom reagovali na kteroukoliv jinou hrozbu ohrožující naší zemi"[128].

V neposlední řadě Čína zastává stanovisko o rozšíření státní suverenity a nezasahování do oblasti kyberprostoru. To znamená, že státy jsou hlavními aktéry v oblasti kyberprostoru, tak jako v reálném fyzickém světě. Rozšíření státní suverenity do oblasti kyberprostoru se řídí následujícími principy[129]:

1) Státy uplatňují svoji svrchovanost v oblasti kyberprostoru nad svými i cizími občany a firmami nacházejícími se na jejich území v rámci svých hranic.

2) Státy by neměly zasahovat do kyberprostoru ostatních států a měly by se zdržet od použití svých zdrojů, kritické infrastruktury a jiných technologiích, aby nedošlo k porušení práv ostatních států.

Čína podporuje myšlenku aktivní kontroly, regulace a monitorování internetu. Usiluje o zlepšení systému řízení internetu, a to prostřednictvím zákonů, veřejného dohledu, vzdělávání, správního dozoru a technické ochrany. Mezi jednotlivé cíle systému řízení internetu patří například umožnění přístupu k internetu široké veřejnosti a usilovat tak o zmenšení digitální propasti mezi jednotlivými regiony a mezi městskými a venkovskými oblastmi. Dále se Čína snaží garantovat občanům svobodu projevu v rámci internetu, podporovat pozitivní a efektivní internetové aplikace, vytvářet spravedlivé tržní prostředí a zajišťovat informační a státní bezpečnost. V rámci mezinárodní spolupráce v oblasti kybernetické bezpečnosti Čína usiluje o zřízení organizace pro řízení internetu na základě demokratických zásad pod záštitou Organizace spojených národů. [130]

Významné čínské úsilí o zavedení norem v kyberprostoru v rámci multilaterální spolupráce a čínský oficiální přístup ke kybernetické bezpečnosti ztělesňuje dokument *The International Code of Conduct for Information Security*[131] předložený Valnému shromáždění v roce 2011. Mezi sponzorující státy dokumentu patří ČLR, Rusko, Tádžikistán, Uzbekistán, Kazachstán a Kyrgyzstán, sdružené země v rámci Šanghajské organizace pro spolupráci.

---

[128] The White House. *International Strategy for Cyberspace*, 2011, str. 14

[129] China Daily.com.cn. *White paper on the Internet in China*, 2010

[130] Tamtéž.

[131] UN General Assembly. *International code of conduct for information security*, 2011

Každý stát se zavazuje k dodržování 11 principů jako je například[132]: respektovat suverenitu, územní celistvost a politickou nezávislost každého státu, dodržovat lidská práva a základní svobody, respektovat práva a svobody v informačním prostoru jako je vyhledávání, získávání a šíření informací za předpokladu dodržování příslušných vnitrostátních právních předpisů, spolupracovat v boji proti trestným a teroristickým aktivitám využívajícím informační a komunikační technologie včetně omezování šíření informací podněcujících terorismus, separatismus či extremismus nebo jinak ohrožujících politickou, ekonomickou a sociální stabilitu států. Desátým principem je podpora OSN jako důležitého aktéra ve formulování mezinárodní norem, mírového řešení sporů a koordinování mezinárodní spolupráce v rámci infomační bezpečnosti. USA, Evropská unie a další západní země nesouhlasí s touto iniciativou vzhledem k odlišnému pohledu na priority v oblasti kyberprostoru, kterými jsou svobodný a otevřený internet a zapojení soukromého sektoru a občanské společnosti při řízení internetu.[133]

Neschopnost dosáhnout dohody v otázkách přístupu k internetu odráží zásadní rozkol mezi západním světem na jedné straně a blokem zemí, především afrických a arabských, SNS v čele s Ruskou federací a ČLR na straně druhé. Tento zásadní rozpor byl viditelný již na Světové konferenci mezinárodních telekomunikací (WCIT-12), která se uskutečnila v prosinci 2012 v rámci Mezinárodní telekomunikační unie (ITU). Na konferenci se řešila především revize stávajícího Mezinárodního telekomunikačního řádu (ITRs), který byl vytvořen v roce 1988. Popudem k revizi byly radikální proměny telekomunikačního trhu důsledkem jeho liberalizace. V rámci konference bylo v plánu jednat i v otázkách přístupu k internetu. Západní země však odmítly jednat o otázkách internetu z důvodu možného přehlasování v oblasti regulace a řízení obsahu internetu, neboť zastávají zcela odlišný přístup k řízení internetu, jež klade důraz na zapojení soukromého i neziskového sektoru po boku vlád. Naopak nezápadní země zastávají státocentrický model řízení internetu. I z tohoto důvodu byla konference neschopná dojít k závěru a finální dokument z jednání nepodepsalo 55 zemí z přítomných 151, počínaje nejvýznamnějšími hráči, jako jsou USA, Kanada, Velká Británie,

[132] The Embassy of PRC in New Zealand. *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*, 2011

[133] FEAKIN, T. *ARF, and how to change the tune of the cyber debate,* 2013

Polsko, Německo a Francie.[134] ČLR okomentovala výsledky jednání následovně: *„Neschopnost WCIT-12 dojít k plnohodnotné dohodě ukazuje omezenou udržitelnost internetové agendy pod dominancí Západu.“*[135]

Podobné napětí existuje také ve snaze o vytvoření mezinárodních norem k řízení internetu. Zatímco autoritářské státy, jako jsou Čína nebo Rusko, usilují o „informační bezpečnost“ včetně otevřené cenzury, jaká by byla v zemích typu Spojených států nemožná, západním demokraciím jde pouze o „kybernetickou bezpečnost“.

Obě mocnosti mají zcela odlišný názor na Úmluvu o kyberzločinu. Čínský odmítavý přístup k Úmluvě zcela odráží její rozvíjející se politiku v oblasti kyberprostoru. Čína odmítla k Úmluvě přistoupit z několika zásadních důvodů: Za prvé, Úmluva odporuje jejímu státocentrickému přístupu k mezinárodním dohodám o kyberprostoru a její zásady by mohly ohrozit suverenitu státu. Za druhé, Úmluva odporuje desátému principu dokumentu *The International Code of Conduct for Information Security*, kde OSN figuruje jako mezinárodní garant v otázkách týkajících se kybernetické bezpečnosti a bezpečného internetu. Současně podle čínského think tanku China Institutes of Contemporary International Relations (CICIR) podporovaném státem může OSN na rozdíl od Rady Evropy lépe odpovídat na potřeby rozvojových států v boji proti potírání kyberzločinu. Spojené státy americké přistoupily k úmluvě v roce 2006 a aktivně se hlásí k jejím zásadám.[136]

I přes rozdílné postoje k politice kyberprostoru našly USA a ČLR společný prostor pro spolupráci. V rámci takzvané Skupiny vládních expertů Group of Government Experts (GGE) pod hlavičkou OSN. Skupina sdružuje 15 států a jejím hlavním úkolem je vyhodnotit existující a potenciální hrozby pocházející z kyberprostoru a nelézt možná opatření k jejich řešení. Výsledkem její činnosti je zpráva *Developments in the Fields of Information and Telecommunications in the context of International Security* potvrzující uplatňování mezinárodního práva na oblast kyberprostoru.

Zpráva odráží čínský státocentrický postoj ke kyberprostoru: *„Státní suverenita a mezinárodní normy a zásady se aplikují na státem prováděné aktivity spojené s informačními*

---

[134] Ministerstvo průmyslu a obchodu. *Výsledek Světové konference o mezinárodních telekomunikacích,* 2012

[135] HSU, K. *China and International Law in Cyberspace*, 2014, str.3

[136] Tamtéž.

a komunikačními technologiemi. ICT infrastruktura nacházející se v daném státě pak podléhá jurisdikci onoho státu.“[137]

Čína souhlasí nejen s uplatňováním mezinárodního práva na oblast kyberprostoru, ale i s užitím specifických stránek mezinárodního práva týkající se státní odpovědnosti, užití vojenské síly a práva ozbrojeného konfliktu. Zpráva je založena na principu mezinárodní spolupráce při zajišťování bezpečnosti a stability a snižování možných rizik. Nástroji k tomu mají být společná opatření mezi něž patří normy, pravidla a zásady zodpovědného chování států. Důležité je rovněž zvyšování transparentnosti zapojením soukromého sektoru a občanské společnosti a budování vzájemné důvěry mezi státy.

Odpovědnost státu

Stát je odpovědný za mezinárodně protiprávní jednání, které mu je přičitatelné. Zpráva výslovně odsuzuje použití proxies k páchání mezinárodně protiprávních činů. Stát by měl usilovat o to, aby jeho území nebylo zneužíváno nestátními aktéry k nezákonnému užití informačních a komunikačních technologií.[138] Jedním ze závěrů zprávy je výrazný posun v uchopení konceptu užití vojenské síly v oblasti kyberprostoru. Zpráva jasně konstatuje uplatnění Charty OSN jako *„nezbytný nástroj k udržení míru a stability a k podpoře otevřeného, bezpečného, mírumilovného a dostupného prostředí informačních a komunikačních technologií.“*[139]

Válečné právo v oblasti kyberprostoru

ČLR sice do určité míry uznává možnost uplatnění válečného práva v kyberprostoru, nicméně konkrétní podmínky jeho ukotvení v této oblasti zůstávají tématem k diskuzi i v ostatních zemích. Na rozdíl od ČLR, Spojené státy jsou toho názoru, že existující mezinárodní normy a smlouvy upravující válečné právo jsou zcela aplikovatelné na oblast kyberprostoru. To znamená, že všechny nové technologie jsou předmětem současného

[137] UNODA. *Report of the Group of Governmental Experts on Developments in the Fields of Information and Telecommunications in the context of International Security,* 2010

[138] UN General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* 2013

[139] Tamtéž.

válečného práva. Uplatnění existujícího válečného práva na oblast kyberprostoru je však sporné, a to ze tří následujících důvodů:

1) Válečné právo nereflektuje realitu současného válčení v kyberprostoru

Podle článku 2 Charty OSN se *„všichni členové vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů“*. Dále dle článku 51 má stát v případě ozbrojeného útoku přirozené právo na individuální nebo kolektivní sebeobranu. Vhledem ke specifickým vlastnostem kyberprostoru a kybernetických útoků je těžké definovat hranici spadající pod ozbrojený útok. Kybernetické útoky mohou mít vážné destruktivní následky bez fyzických škod či obětí. Například nenásilné kybernetické útoky, jako je krádež dat či systémová sabotáž, mohou ohrozit základní bezpečnostní zájmy státu, aniž by přitom způsobily fyzickou škodu, tak jako tradiční ozbrojené útoky.

2) *Nedostatečné mezinárodně právní ukotvení*

Zásadním problémem je nedostatečná spolupráce mezi státy v oblasti vymáhání práva. Vzhledem k absenci všeobecně platných definic jako je užití síly, ozbrojený útok nebo kybernetická špionáž v mezinárodně závazné smlouvě, zvyšuje pravděpodobnost, že se státy dopustí pochybení jak na takové hrozby reagovat. Přehnané reakce by pak mohly vést k nechtěné eskalaci konfliktů. Státy se tak více spoléhají na své instinkty a hodnotí případ od případu místo toho, aby jednaly podle závazného postupu ukotveného v mezinárodní smlouvě. Taková ad hoc řešení pak stěží zabrání postupné militarizaci kyberprostoru. Institucionalizace mezinárodní spolupráce v potírání kyberzločinu usnadní stíhání pachatelů a ztíží jejich činnost. Úmluva o kyberzločinu jako zatím jediný závazný mezinárodní nástroj poskytuje pevný základ pro potírání kyberkriminality. Jejím nedostatkem zůstává počet signatářských zemí (50 států) a absence takových hráčů, jako je Čína a Rusko.

3) Charakter kyberprostoru

Samotný charakter kyberprostoru, pro který jsou typické téměř neomezené hranice vstupu a obtížné odhalovaní potenciálních pachatelů, z něj vytváří příznivé prostředí pro

páchání kybernetických útoků nízké intenzity. I když přičitatelnost trestného kybernetického činu je složitá, není zcela vyloučená a v současné době může být prováděna i nevládními subjekty. Překážkou k úspěšnému stíhání je nedostatečná součinnost mezi státy při vyšetřování. Příkladem takové soukromé firmy vyšetřující kybernetickou trestnou činnost je bezpečnostní společnost Mandiant, která odhalila konkrétní členy speciální jednotky 61398 v Šanghaji, na které FBI vydala zatykač. Pokud se z kyberprostoru stane zóna neustálých konfliktů, civilní dimenze kyberprostoru se zcela vytratí a s nimi i komerční a sociální výměna, kterou ICT přináší.

6 Sino-Americká krize a válka

Jak USA, tak Čína považují v současné době kybernetické operace za nezbytnou součást vedení boje.[140] Cílem kybernetických útoků jsou kritická národní, vládní a komerční infrastruktura a v neposlední řadě samozřejmě internet. Vzhledem ke zranitelnosti civilní internetové sítě si oba státy uvědomují, že vést kybernetickou vojenskou operaci proti C4ISR nepřítele bez překročení do civilní domény, vyžaduje ohromnou politickou kontrolu, neboť by tím mohly spustit otevřenou a možná i nekontrolovatelnou kybernetickou válku.

V dohledné době je velmi pravděpodobné, že se kybernetické válčení lépe začlení do širších vojenských schopností obou států. Nasvědčuje tomu význačný nárůst instituce US Cyber Command (až 6000 osob podle plánu).[141] Dochází k institucionalizaci kyberválky v rámci národní strategie. Na kyberprostor se již nenahlíží jako na zvláštní oblast pro vedení konfliktu, ale jako na oblast válčení vedle země, moře, vzduchu či vesmíru. Rostoucí závislost vojenských sil a misí na počítačových sítích – čínská strategie „anti-access a area-denial" (A2/AD) a naopak americký koncept „Air-Sea Battle", dává oběma státům silný podnět k tomu začít kybernetickou válku. Strach, že druhá strana zasáhne první, nevyhnutelně vede k závodu ve zbrojení. Kybernetické válčení může být považováno za relativně jednoduchý způsob, jak s nízkým rizikem ochromit systémy nepřítele. Faktory, které můžou vést k eskalaci konfliktu mezi USA a Čínou jsou: čínská a americká vojenská strategie preferující „první úder", minimální hranice pro zahájení útoku v oblasti kyberprostoru a vzájemná možná spojitost mezi kybernetickým a konvenčním válčením.

6.1 Americko-čínský konflikt v roce 2001

Dne 1. dubna 2001 došlo k vážné kolizi mezi americkým průzkumným letounem EP-3 a čínským stíhacím letounem F-8 nad Jihočínským mořem. Čínský pilot srážku nepřežil a americká posádka byla nucena nouzově přistát na ostrově Hainan, kde byla zadržena čínskou vládou po dobu 11 dnů. Letoun EP-3, vybavený vyspělou tajnou komunikační a

[140] GOMBPERT D. a LIBICKI M. *Cyber Warfare and Sino-American Crisis Instability,* 2014

[141] Tamtéž.

zpravodajskou technikou, byl podroben detailnímu technickému zkoumání. Vznikla velmi napjatá politická situace ústící v intenzivní diplomatická jednání. Obě mocnosti měly odlišný názor na příčinu nehody a propuštění zadržované posádky. Čína silně odsoudila americkou vládu za narušení jejího vzdušného prostoru a suverenity. Čínští představitelé požadovali oficiální omluvu po Spojených státech za zavinění srážky a s tím související právo na inspekci letadla.[142] Spojené státy se měly veřejně omluvit čínské vládě a čínskému lidu. Vyhověním žádosti o omluvu vyjádřenou slovem „apology", které má jednoznačný výraz, by však pro Spojené státy znamenalo, že oficiálně přiznávají odpovědnost za incident. Prezident Bush ve svém vystoupení vyjádřil lítost nad ztrátou čínského pilota a letadla a zároveň vyjádřil přesvědčení, že incident by neměl destabilizovat vzájemné vztahy. Bushova administrativa se od počátku odmítla za incident omluvit, jak požadovala čínská strana, a vzít tak na sebe plnou zodpovědnost.[143]

Až dopis zaslaný 11. dubna americkým velvyslancem přesvědčil čínskou vládu, aby posádku propustila. Obsahoval vyjádření upřímné lítosti nad ztrátou čínského pilota a letadla, aniž by v něm bylo použito slovo „apology", které má jednoznačný překlad omluvy. Spojené státy se v něm také omluvily za to, že jejich letoun byl nucen nouzově přistát a tím vstoupil do čínského vzdušného prostoru bez souhlasu. Čínská vláda přijala dopis a souhlasila s propuštěním americké posádky. Nicméně vznesla požadavek o ukončení průzkumných letů poblíž svého pobřeží.[144] Pro čínskou veřejnost byl americký projev lítosti „very sorry" médii interpretován jako „apology" a tudíž považován za úplnou omluvu, kterou Čína požadovala od počátku. Slovní spojení upřímné lítosti nad ztrátou pilota a letadla bylo považováno za politování nad celým incidentem. Tím si čínská vláda nejen zachovala tvář před vlastním obyvatelstvem, ale rovněž předešla přímé konfrontaci, která by mohla narušit vzájemné vztahy se Spojenými státy.[145]

Tvrdý americký postoj byl mezi čínským lidem vnímán jako arogantní akt hegemona a vedl k vlně antiamerických aktivit. Na rozdíl od masivních demonstrací před americkou ambasádou a konzuláty následujících po neúmyslném vybombardování čínské ambasády v Bělehradě v roce 1999, čínští občané vyjádřili svou nespokojenost a silné emoce skrz

---

[142] CRS Report for Congress. *China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications,* 2001

[143] Tamtéž.

[144] Tamtéž. str. 4-6

[145] ZHAO S. *Chinese Pragmatic Nationalism and Its Foreign Policy Implications,* 2008

masmédia. Mezinárodní veřejnost se silně přikláněla k čínské straně a dokonce podle online průzkumu časopisu Time 77% dotázaných Američanů bylo toho názoru, že USA by měly převzít hlavní odpovědnost za incident.[146] Výsledky tohoto průzkumu byly velmi medializovány na čínské straně. Čínská veřejnost byla incidentem velmi pobouřena, což se odráželo na internetových fórech; viníkem nehody byly USA, jejichž průzkumné letadlo nezákonně vstoupilo do čínského vzdušného prostoru za účelem špionáže, čímž ohrozilo národní bezpečnost, a čínský letoun tak byl nucen letadlo zastavit. Viníkem byl americký pilot, který svým prudkým manévrem způsobil kolizi.[147]

Napjatá politická situace byla rovněž doprovázena vzrůstajícím počtem kybernetických útoků. Kenneth Geers uvádí, že *„téměř vše, co se odehrává ve skutečném světě, se odráží i v tom kybernetickém. Měli bychom tedy počítat s tím, že určitá část každého politického či vojenského konfliktu se může současně odehrávat také na Internetu, což může být stejně tak důležité jako události odehrávající se mimo kyberprostor.“*[148] Mezi oběma zeměmi docházelo k vzájemným kyberútokům a defacementům webových stránek. Obě strany byly navíc podporovány skupinami hackerů po celém světě. Čínští hackeři jako Honker Union of China a China Eagles na protest proti americkému hegemonnímu jednání[149] organizovali rozsáhlé a vytrvalé útoky na americké webové stránky.

Masivní akce hackerů vedly k tomu, že americké Národní centrum ochrany infrastruktury (National Infrastructure Protection Center - NIPC) vydalo varování o zvýšené aktivitě hackerů proti americkým systémům v období od 30. dubna až 7. května 2001. Narůstající počet útoků během tohoto období také souvisí s významnými dny pro ČLR, jako je 1. května Svátek práce, 5. května Den mládeže či výročí neúmyslného vybombardování čínské ambasády americkými jednotkami v Bělehradě v roce 1999.[150] Na 4. května 2001 rovněž připadá 82. výročí Hnutí čtvrtého května symbolizujícího vzestup čínského nacionalismu a protestujícího proti cizí nadvládě. Nacionalismus představuje velmi účinný nástroj komunistické strany, neboť pocity křivdy z nadvlády cizích mocností je hluboce zakořeněný v čínské společnosti. Ústředním motivem každého významného politického

---

[146] LIEW, L. a VANG, S. *Nationalism, Democracy and National Integration in China*, 2012

[147] Tamtéž.

[148] GEERS K. *Cyberspace and the Changing Nature of Warfare,* 2008

[149] People`s Daily. *Domineering Action and Hegemonic Logic*, 2001

[150] The Information Warfare Site. *"Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May",* 2001

představitele 20. století bylo tudíž obnovit právoplatné místo Číny mezi národními státy; vše pramenilo ze sdílené hořkosti k cizím mocnostem, které způsobily její ponížení.[151]

Následkem vyhrocené politické situace začala kybernetická válka mezi oběma skupinami hackerů. Čínští hackeři vytvořili nový server KILL_USA spolu s odkazy na volně stažitelné programy umožňující útoky na americké servery. Američtí hackeři reagovali na akce pro-čínských hackerských skupin vytvořením obdobného serveru KILL_CHINA s obdobným obsahem určeným pro útoky naopak na čínské servery. Plánování a organizování útoků na obou stranách probíhalo přes různá internetová diskuzní fóra a IRC. [152]

Napadené stránky obsahovaly čínské vlajky, politické slogany a fotografie pohřešovaného čínského pilota. Útoky lze považovat za vlastenecky motivované. *„My, čínský lid hluboce milujeme naši zemi a její obyvatele. Jsme rozhořčeni imperialistickými snahami cizích států a pokud bude třeba, jsme připraveni naší zemi obětovat, co bude třeba, včetně našich životů.“*[153]

New York Times označil americko-čínský konflikt jako „World Wide Web War I.; první světovou hackerskou válku.[154] Tato situace představovala klasický případ konfliktu, jehož příčinou byl fyzický střet s následky odehrávající se v kyberprostoru. Jednalo se rovněž o politicky motivovaný hacking jakožto formu protestu, která se stává díky internetu mnohem lépe dostupnou. Každému uživateli internetu stačí jednotýdenní tréning, aby ovládal základy hackingu. Výhodou je, že poselství zainteresovaných skupin může prostřednictvím internetu oslovit širokou skupinu populace. Americký internetový bezpečnostní expert Jeff Moss dodává, že trend politického hackingu bude nadále stoupat a žádná legislativa to nemůže zastavit, neboť se jedná především o problém technický.[155]

---

[151] ZHAO, S. *Chinese Pragmatic Nationalism and Its Foreign Policy Implications,* str. 5-6, 2008

[152] JIROVSKÝ, V. *Kybernetická kriminalita,* 2007

[153] CNN. *Feds warn of May Day attacks on U.S. Web sites,* 2001

[154] SMITH, C. *May 6-12; The First World Hacker War*, 2001

[155] TANG, R. *China-U.S. cyber war escalates*, 2001

6.2 Kybernetické špionážní aktivity Číny proti americkým cílům

V březnu 2013 vydala americká bezpečnostní firma Mandiant podrobnou šedesátistránkovou studii[156] o velmi aktivní skupině hackerů provádějících kybernetickou špionáž proti americkým cílům. Studie popisuje rozsáhlou síť kybernetických útoků proti americkým obchodním společnostem, organizacím a vládním agenturám, které pocházejí z tzv. jednotky č. 61398 sídlící pravděpodobně v budově na okraji Šanghaje, jež patří čínské lidové armádě. Formálně tento útvar ve vojenských materiálech neexistuje. Firma nebyla schopná detekovat hackery přímo do budovy, ale je si zcela jistá, že neexistuje jiné věrohodnější vysvětlení, proč by se jinak takové množství digitálních stop koncentrovalo na tomto konkrétním území. Čína opakovaně odmítá jakoukoliv odpovědnost za prováděné útoky. Zakladatel firmy Mandiant Kevin Mandia to komentuje slovy *„buď útoky vycházejí z jednotky 61398, nebo lidé, kteří spravují nejvíce monitorovaný a kontrolovaný internet na světě, nemají žádné tušení o tom, že tisíce osob provádí útoky z této čtvrti.“*[157]

Americká vláda opakovaně sdílela s čínskými představiteli své obavy ohledně kybernetické krádeže dat. Diskuze probíhaly na nejvyšší úrovni. Nicméně z diplomatických důvodů nebyla skupina hackerů záměrně spojována s čínskou armádou. Cílem zprávy Mandiant bylo veřejně upozornit na rozsah a dopad kybernetických aktivit této jednotky. Cílem čínské jednotky byly technologické plány, výrobní postupy, výsledky klinických testů, vyjednávací strategie a další chráněné informace z více než 20 průmyslových odvětví. Nejnovější útoky se podle zprávy snažily získat přístup k americké kritické infrastruktuře, jako je rozvod vody, plynu a elektřiny. Jedním z takových útoků byla napadena společnost Telvent, v současnosti vlastněna firmou Schneider Electric, jež navrhuje software, který umožňuje provozovatelům ropovodů, plynovodů a rozvodné sítě vzdálený přístup k ventilům, spínačům nebo bezpečnostním systémům. Talvent disponuje detailními plány a přístupem do systémů více než 60 % ropovodů a plynovodů v Severní a Jižní Americe. Podle zprávy se jednotce povedlo napadnout firmu Talvent a ukrást jí potřebná data k získání přístupu do systémů, nicméně jejich přístup byl ihned odříznut.[158]

---

[156] MANDIANT. *APT1: Exposing One of China's Cyber Espionage Units*, 2013

[157] SANGER, D. - BARBOZA, D. – PERLROTH, N. *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, 2013

[158] Tamtéž.

Americká vláda plánuje účinnější obranu proti opakovaným útokům na kritickou infrastrukturu a čínským hackerským skupinám, a to například prostřednictvím prezidentského nařízení, které se týká sdílení informací mezi internetovými poskytovateli a vládou.[159]

V květnu 2013 americké ministerstvo obrany poprvé obviňuje čínskou vládu a armádu z přímé účasti na provádění kybernetické špionáže proti americkým cílům.[160] Zpráva ministerstva obrany Spojených států amerických z roku 2013 týkající se vojenského a bezpečnostního vývoje v ČLR (*Annual Report to Congress: Military and Security Developments Involving the People's Republic of China states 2013*) uvádí, že během roku 2012 došlo k mnoha neoprávněným proniknutím do počítačových systémů po celém světě – včetně těch amerických, přičemž podle všeho lze tyto neautorizované přístupy přičíst přímo čínské vládě a armádě. Průniky byly provedené formou vytěžování počítačové sítě (CNE). Zpráva dále upřesňuje, že takto získané informace může Čína využít ve svém vojenském nebo high-tech zpracovatelském průmyslu. Vojenští plánovači mohou zneužít v případě krize, kdy je stát nejvíce oslaben, informace o americké obranné síti a logistice, a tím lépe určit možnosti amerických vojenských schopností. Zneužity mohou být taktéž neoficiální informace americké vlády týkající se její zahraniční strategie vůči Číně. Zpráva závěrem konstatuje, že přístupy a dovednosti k provedení těchto neoprávněných průniků jsou obdobné k provádění CNA.[161]

Předešlé dokumenty ministerstva obrany USA pouze odkazovaly na to, že průniky a krádeže dat pocházejí z Číny. Americká vláda udělala zásadní krok v tom, že veřejně označila čínskou vládu a armádu za původce kybernetické špionáže. Čínská vláda však jakékoliv zapojení v kybernetické špionáži proti Spojeným státům popírá s poukazem na anonymitu, kterou kyberprostor nabízí a na nedostatek prokazatelných forenzních dat.[162]

---

[159] The White House. *Executive Order -- Improving Critical Infrastructure Cybersecurity*, 2013

[160] *2013 Report to Congress of the U.S.-China Economic and Security Review Commission*, 2013: str. 245

[161] Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China states 2013*, 2013: str. 36

[162] *2013 Report to Congress of the U.S.-China Economic and Security Review Commission*, 2013: str. 245-246

6.3 Případ Edwarda Snowdena

Edward Snowden je bývalý externí pracovník americké Národní bezpečnostní agentury (NSA) a Ústřední zpravodajské služby (CIA), který tisku vyzradil informace o utajovaném rozsáhlém odposlouchávání elektronické komunikace ze strany amerických bezpečnostních služeb. Program PRISM řízený Národní bezpečnostní agenturou údajně umožňoval přímý přístup k informacím a sběr dat, jako je historie vyhledávání, obsah emailů, přenosy souborů, živé chaty a další.[163] Odposlouchávání probíhalo ve spolupráci s velkými americkými firmami Microsoft, Google a Facebook. Internetoví giganti svoji účast na programu popírají.[164] Snowden rovněž vyzradil, že americká vláda takto sledovala i své vlastní občany.[165] V reakci na kompromitující články vydala americká vláda prohlášení v němž uvádí, že odposlouchávání elektronické komunikace probíhá v souladu s nařízením FISA (the Foreign Intelligence Surveillance Act).[166] Podle prohlášení články obsahují četné nepřesnosti. Získané informace v rámci programu FISA slouží k ochraně národa před řadou hrozeb. Sledování se v rámci programu zaměřuje pouze na osoby pobývající mimo území Spojených států.[167] *„Zpravodajské aktivity nemohou být záměrně namířeny proti kterémukoliv americkému občanovi, nebo jiné osobě nacházející se na území Spojených států.“* [168]

---

[163] GREENWALD, G. a MACASKILL, E. *NSA Prism program taps in to user data of Apple, Google and others*, 2013

[164] Technnet.cz *Zprávu o sledování lidí na internetu vynesl bývalý technik CIA. Utekl z USA*, 2013

[165] LAM, L. *Edward Snowden: US government has been hacking Hong Kong and China for years*, 2013

[166] The Foreign Intelligence Surveillance Act z roku 1978 stanovuje postupy pro podávání žádostí o soudní povolení týkající se elektronického odposlouchávání a fyzického sledování osob zapojených do špionážních aktivit nebo mezinárodního terorismu namířeného proti Spojeným státům ze strany jiné mocnosti. O žádostech rozhoduje speciální soud pro to určený (Federation of American Scientists. *Foreign Intelligence Surveillance Act*, 2014).

[167] Office of the Director of National Intelligence. *DNI Statement on Activities Authorized Under Section 702 of FISA*, 2013

[168] Tamtéž.

Snowdenovi hrozí trestní stíhání za krádež vládního majetku, neoprávněné předávání informací o národní bezpečnosti a vědomé vyzrazení tajných informací.[169]

Snowden dále poskytl interview pro noviny South China Morning Post v Hongkongu, kde se přechodně skrýval. V interview odhalil, že v rámci kontroverzního programu americké vlády docházelo od roku 2009 k pronikání do počítačů v Hongkongu a Číně. Hlavními cíli byly politici, podnikatelé a studenti. Snowden se domníval, že celkový počet kybernetických operací přesahoval 61 000, z nichž stovka byla namířena na hongkongské a čínské cíle.[170]

6.3.1 Dopad případu Snowden na úsilí USA zastavit čínskou kyberšpionáž

Vyzrazení tajných dokumentů o programu PRISM podstatně ovlivnilo úsilí americké diplomacie přimět Čínu, aby omezila své kybernetické aktivity namířené proti americkým společnostem. Americko-čínský dialog týkající se kybernetické bezpečnosti představuje největší výzvu v bilaterálních vztazích mezi mocnostmi. Čínští představitelé chtějí zachovat stabilitu ve vzájemných vztazích a proklamují, že kybernetická bezpečnost by se neměla stát hlavní příčinou jejich vzájemného napadání a zdrojem napětí, ale naopak odrazovým můstkem v jejich vzájemné spolupráci.[171] Nicméně skandál poskytl příležitost čínským státním médiím k přesvědčení občanů, že jejich vláda dodržuje nejvyšší morální principy, co se týče problematiky internetu.[172] Státní čínská zpravodajská agentura Xinhua veřejně prohlásila, že zatímco si „*Spojené státy dlouhou dobu hrály na oběť kybernetických útoků, ve skutečnosti se ukázalo, že jsou samy největším strůjcem těchto útoků*.“[173] Mluvčí čínského ministerstva obrany Yang Yujun se k případu Snowdena vyjádřil následovně: *„Případ Prism gate[174] stejně jako prisma odráží skutečnou tvář a pokrytecké činy země, která zneužívá své výsadní postavení v informačních technologiích k obohacení se a zároveň vznáší nepodložená*

[169] BBC. *Profile: Edward Snowden*, 2013

[170] LAM, L. *Edward Snowden: US government has been hacking Hong Kong and China for years*, 2013

[171] MCGREGOR, R. *Obama and Xi talks tackle cyber security*, 2013

[172] BUCKLEY, Ch. *Chinese Defense Ministry Accuses U.S. of Hypocrisy on Spying*, 2013

[173] DYER, G. a HILLE, K. *US shrugs off Snowden leaks to press Beijing on cyber theft*, 2013

[174] Označení “prism gate“ užívají čínská média.

obvinění proti ostatním zemím. Tento dvojí metr podkopává stabilitu a mír v kyberprostoru.“[175]

6.4 Obvinění pěti čínských vojenských hackerů z kyberšpionáže

V květnu 2014 americké ministerstvo spravedlnosti obvinilo pět čínských armádních hackerů, kteří se dopustili kybernetické špionáže na amerických společnostech a odborovém svazu. Je to vůbec první případ obvinění jednotlivců, kteří podnikali nelegální kybernetické aktivity ve službách a z příkazu jiného státu. Náměstek generálního prokurátora pro národní bezpečnost John Carlin dodává, že *„státní aktéři zapojení do kyberšpionáže nemohou být imunní vůči zákonům jen proto, že se schovávají za vlajku své země. Kybernetická krádež je skutečná krádež a státem podporovaní kyberzločinci se budou za své činy zodpovídat.“*[176] 31 bodů obžaloby vznesené proti pětici hackerů zahrnuje: spiknutí za účelem spáchání počítačového podvodu, neautorizovaný přístup k počítači pro účely obchodního prospěchu a finančního obohacení se, poškození počítače přenosem kódu a příkazy, páchání činů prostřednictvím krádeže identity, ekonomickou špionáž a krádež obchodních tajemství. Obviněna byla pětice důstojníků čínské lidové armády náležících k jednotce 61398 - Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui.[177] Obvinění jsou vinni ve všech bodech obžaloby. Případné tresty se pohybují do 15 let odnětí svobody. Nejvyšší trest, 15 let, může být udělen za ekonomickou špionáž.[178]

Šest amerických společností bylo napadeno v době, kdy vedly jednání, join ventures nebo právní kroky se státními podniky v Číně. Pachatelé se měli dopustit krádeže chráněných informací, jako je například historie zaměstnaneckých emailů nebo technické specifikace a

---

[175] Defense Ministry spokesman Yang Yujun's regular press conference on June 27, 2013," Ministry of National Defense of the People's Republic of China, July 2, 2013. *In*: SWAINE, M. *Chinese Views on Cybersecurity in Foreign Relations,* 2013

[176] The FBI. U*.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, 2014

[177] The FBI. *Cyber's Most Wanted*, 2014

[178] The FBI. U*.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, 2014

nákresy jaderné elektrárny[179]. Mezi oběti útoků patří například firma Westinghouse Electric Co., United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATI) a další. Americký generální prokurátor Eric Holder se k případu vyjádřil následovně: *„Úspěch na globálním trhu by měl spočívat na schopnostech firmy inovovat a utkat se s konkurencí, nikoliv na tom, že vláda poskytne prostředky ke špionážím a krádežím cizích obchodních tajemství. Americká vláda nebude tolerovat ilegální aktivity kteréhokoliv národa vedoucí k podkopání integrity spravedlivé hospodářské soutěže a fungování volného trhu.“*[180]

Čínské ministerstvo zahraničí okamžitě reagovalo na vznesená obvinění tím, že pozastavilo aktivity v rámci čínsko-americké pracovní skupiny a požadovalo po Spojených státech okamžité stažení obvinění, která jsou podle něj postavená na vykonstruovaných tvrzeních. Mluvčí ministra zahraničí Qin Gang dodává, že *„stíhání pěti důstojníků je vážné porušení mezinárodního práva a poškozuje vzájemnou spolupráci a důvěru mezi mocnostmi“.*[181] Dále se odkazuje na předchozí odhalení americké vlády, která sama prováděla rozsáhlou kybernetickou špionáž proti čínským cílům. Čína opakovaně vyžaduje jasné vysvětlení a ukončení těchto činností z americké strany (monitorování sítě, sledování, organizovaná krádež).[182]

Následně reaguje i čínské ministerstvo obrany, které ve svém prohlášení jednoznačně popírá, že by se čínská lidová armáda účastnila kybernetické špionáže proti americkým cílům. A téměř identicky jako ministerstvo zahraničí odkazuje na aktivity Spojených států: *„Spojené státy již dlouhou dobu disponují vyspělou technologií, pomocí níž prováděly rozsáhlé sledování zahraniční vlád, firem a osob. Toto pokrytectví a nastavování dvojích standardů, co se týče kybernetické bezpečnosti, je dobře známý fakt, který odhalily incidenty WikiLeaks a Edward Snowden.“*[183] Podle ministerstva čelila armádní síť několika útokům pocházejícím podle IP adresy ze Spojených států. Prohlášení závěrem nabádá Spojené státy k ukončení

---

[179] The FBI. U.*S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, 2014

[180] Tamtéž.

[181] Ministry of Foreign Affairs of the People`s Republic of China. *China strongly attacks the United States "to prosecute" Chinese officials*, 2014

[182] Tamtéž.

[183] Ministry of National Defense of the People`s Republic of China. *Defense Ministry spokesman Geng Yansheng's Remarks on the US Justice Department to prosecute Chinese soldiers*, 2014

těchto aktivit. Dále mají Spojené státy podniknout konkrétní kroky, aby dostály svému slibu o budování stabilní a spolehlivé vzájemné vojenské spolupráce.[184]

6.4.1 Případ Su Bin

Americké ministerstvo spravedlnosti obvinilo čínského podnikatele v leteckém průmyslu, jehož firma sídlí v Kanadě, z průmyslové špionáže. Su Bin je čínský občan žijící v Kanadě, který se měl nabourat do počítačové sítě klíčových leteckých dodavatelů, včetně Boeingu (the Boeing Company), který rovněž vyrábí vojenský transportní letoun C-17. Su Bin byl na základě žádosti ze Spojených států zadržen v Kanadě a nyní se nachází ve vazbě a čelí extradici do Spojených států. Podle padesátistránkového trestního oznámení měl Su Bin další dva komplice působící v Číně a spolu s nimi se měl nabourat do počítačových systémů a zcizit tajné informace a technické specifikace nejmodernějších stíhacích letounů F-22, F-35 a již zmíněného transportního letounu C-17. Mezi body obžaloby patří neautorizovaný přístup do počítačové sítě, spolčení za účelem krádeže obchodních tajemství a postoupení získaných informací třetí osobě. Za vznesená obvinění hrozí Su Binovi trest odnětí svobody v maximální výši 30 let.[185]

Na rozdíl od pěti vojenských důstojníků obviněných v květnu z kybernetické špionáže proti americkým společnostem, Su Bin podle trestního oznámení pracoval pro své vlastní finanční obohacení. Mnoho hackerů v Číně pracuje na volné noze nebo ve svém volném čase a následně se snaží ilegálně získané informace prodat státem vlastněným firmám. Prodej ukradených plánů nebyl vždy jednoduchý, jak také naznačuje emailová korespondence mezi hackerem a Su Binem*: „Rozumím, že je to pro Vás velmi naléhavé, ale není jednoduché tyto informace prodat.“* [186] Su Binovi komplici cílili především na technologie vojenské zpravodajské služby a Su Bin následně třídil, které informace budou zajímavé pro čínské

---

[184] Ministry of National Defense of the People`s Republic of China. *Defense Ministry spokesman Geng Yansheng's Remarks on the US Justice Department to prosecute Chinese soldiers*, 2014

[185] The FBI. *Los Angeles Grand Jury Indicts Chinese National In Computer Hacking Scheme Allegedly Involving Theft Of Trade Secrets*, 2014

[186] GROSSMAN, A. a YADRON, D. *U.S. Accuses Chinese Executive of Hacking to Mine Military Data*, 2014

firmy.[187] I když je americká vláda plně odhodlána bojovat proti ekonomické špionáži, přesto se v tomto případě pečlivě vyvarovala obvinit čínskou vládu, že stojí za zločinem, aby předešla incidentu s Pekingem. Civilní případ může mít silnější právní dopad, než je tomu u pěti obviněných čínských vojáků, kde je nulová šance, že budou vydáni do Spojených států.[188]

Je velmi nepravděpodobné, že i přes úsilí Spojených států donutit Čínu k odpovědnosti za kybernetickou špionáž, změní Čína svůj postoj k této problematice. Čína opakovaně odmítá jakékoliv zapojení do kybernetické špionáže proti Spojeným státům a naopak nabádá k bilaterální a multilaterální spolupráci při sestavení pravidel v oblasti kybernetické bezpečnosti. Spolupráce v rámci pracovní skupiny o kyberbezpečnosti nevede k žádnému pokroku a navíc téma špionáže bylo smeteno ze stolu. Naproti tomu obě mocnosti budují ofenzivní a defenzivní kybernetické kapacity vůči sobě navzájem, což vede pouze k závodu ve zbrojení a zvyšující se nejistotě. [189] Aféra Edwarda Snowdena ztížila vyjednávací pozici Spojených států. Jakékoliv snahy o zastavení těchto aktivit proti Spojeným státům zůstávají na mrtvém bodě a to z několika důvodů: mezinárodní právo nepovažuje špionáž za protizákonnou, charakter kyberprostoru umožňuje provádět aktivity přes různé IP adresy a pachatele lze jen stěží vypátrat a následné potrestání konkrétních viníků je rovněž těžko proveditelné, neboť jako tomu bylo v případě čínských vojáků, existuje nulová šance, že by pachatelé byli vydáni pro soudní řízení a vykonání trestu.[190]

---

[187] GROSSMAN, A. a YADRON, D. *U.S. Accuses Chinese Executive of Hacking to Mine Military Data*, 2014

[188] TIEZZI, S. *The New US Court Case Against Chinese Hacking*, 2014

[189] SWAINE, M. *Chinese Views on Cybersecurity in Foreign Relations,* 2013: str. 1

[190] ABC. *China leads the world in hacking*, 2014

Závěr

Teoretický rámec zkoumání kybernetické bezpečnost byl založen na teorii rozšířeného pojetí bezpečnosti Kodaňské školy. Klíčových pět sektorů bylo rozšířeno o šestý, kybernetický sektor. Rozšíření konceptu lze chápat jako nezbytný předpoklad pro systematickou analýzu kybernetické bezpečnosti. Kybernetický sektor bezpečnosti popisuje ochranu informačních systémů, které jsou nutnou podmínkou pro fungování všech lidských aktivit v současném informačním věku. Tradiční interakcí v tomto sektoru je šíření a výměna informací a základním cílem pak zachování důvěrnosti, dostupnosti a integrity informací. K nejvýraznějším hrozbám patří vážné narušení kritické infrastruktury státu, kyberšpionáž, krádež tajných informací a obchodních tajemství, duchovního vlastnictví, hacktivismus a další kriminální činnosti. Ačkoliv bylo řečeno, že kybernetický sektor není zaveden jako všeobecně uznávaný pojem v terminologii Kodaňské školy, a jedná se spíše o sumu vybraných jevů, které se týkají kybernetické bezpečnosti a jejích aktérů, z hlediska současného významu informačních a komunikačních technologií jej však můžeme považovat za svébytnou jednotku.

Komparací čínského a amerického přístupu ke kyberprostoru bylo zjištěno, že obě země mají zcela odlišný pohled na danou problematiku. Sledované země se různí v otázce řízení internetu, což se odráží ve snahách o vytvoření mezinárodních norem upravujících kyberprostor. Zatímco Čína nebo Rusko usilují o informační bezpečnost včetně otevřené cenzury internetu, Spojené státy a jiné západní demokracie o kybernetickou bezpečnost. Cenzura by v západních zemích nebyla možná, neboť lidé považují internet za prostor, kde se mohou svobodně vyjádřit a jakákoliv restrikce internetu by byla vnímána jako narušení tohoto práva. Čína disponuje nejdůmyslnějším režimem kontroly internetu a toku informací na světě. Tzv. Great Firewall of China je navržen tak, aby fakticky oddělil čínský kyberprostor od zbytku světa. Na sociální sítě, kde dochází k vzájemné interakci mezi uživateli, Čína nahlíží jako na zdroj chaosu a politické destabilizace státu. Hlavním cílem kontroly internetu a toků informací je zachování čínského politického systému pod dominancí komunistické strany.

Rozdílný přístup obou vlád k úloze státu v oblasti kybernetické bezpečnosti představuje hlavní překážku v sestavení mezinárodních norem, které by upravovaly tuto oblast. Spojené státy spolu ze zbytkem západního světa se stavějí negativně k legitimizaci cenzury internetu. Na druhou stranu ČLR obviňuje Spojené státy z nastavování dvojích standardů, přičemž poukázala na odhalení Edwarda Snowdena, kdy Spojené státy samy

kontrolují internet, aktivity cizích vlád, a dokonce své vlastní občany v rámci programu PRISM. Iniciativou ze strany ČLR týkající se zavedení norem v kyberprostoru v rámci multilaterální spolupráce je dokument *The International Code of Conduct for Information Security*. Přičemž nejdůležitějším aktérem zaštiťujícím mezinárodní spolupráci v rámci kybernetické bezpečnosti by měla být OSN. Iniciativa odráží čínský oficiální přístup ke kybernetické bezpečnosti, čímž je zejména uplatňování státní suverenity na tuto oblast a kontrola, regulace a monitorování internetu. USA spolu s EU a dalšími západními zeměmi nesouhlasí s touto iniciativou vzhledem k odlišným prioritám v oblasti kyberprostoru. Důvodem je zejména řízení internetu, do kterého by vedle samotného státu měl být zapojen rovněž soukromý sektor a občanská společnost kvůli zajištění větší transparentnosti. Spojené státy se aktivně hlásí k zásadám Úmluvy o kyberzločinu Rady Evropy, která představuje první mezinárodněprávní nástroj určený k řešení problémů v oblasti počítačového zločinu s mezinárodním přesahem. Odmítavý postoj k Úmluvě ze strany Číny zcela odráží její rozvíjející se politiku v oblasti kyberprostoru. Úmluva neodráží čínský státocentrický pohled v oblasti kyberbezpečnosti a její zásady by mohly ohrozit suverenitu státu. V Úmluvě nefiguruje OSN jako hlavní garant. To je důležitým momentem, neboť podle čínského pohledu může OSN na rozdíl od Rady Evropy lépe odpovídat na potřeby rozvojových států v boji proti potírání kyberzločinu.

Ve vojenské oblasti považují obě země kybernetické operace za nezbytnou součást boje. Rostoucí závislost vojenských sil a misí na počítačových sítích, dává oběma státům silný podnět k tomu začít kybernetickou válku. Dochází k institucionalizaci kybernetické války v rámci národních strategií mocností. Státy se rozcházejí v otázkách uplatnění válečného práva v kyberprostoru. ČLR sice do určité míry uznává možnost uplatnění válečného práva v kyberprostoru, nicméně konkrétní podmínky jeho ukotvení zůstávají tématem k diskuzi. Na rozdíl od ČLR jsou Spojené státy toho názoru, že existující mezinárodní normy a smlouvy, které upravují válečné právo, jsou zcela aplikovatelné na oblast kyberprostoru. To znamená, že všechny nové technologie jsou předmětem současného válečného práva. Uplatnění existujícího válečného práva na oblast kyberprostoru je však sporné. Válečné právo totiž nereflektuje realitu současného válčení v kyberprostoru. Kybernetické útoky mohou mít například vážné destruktivní následky bez fyzických škod či obětí, které jsou typické pro tradiční ozbrojené útoky. Samotný charakter kyberprostoru rovněž znesnadňuje aplikovatelnost současného válečného práva. Jedná se především o rozlišení mezi kybernetickou špionáží na jedné straně a kyberzločinem a vojenskými kybernetickými aktivitami na straně druhé. Je totiž velmi obtížné se vůbec dopátrat, zda je

pachatelem stát či kriminální skupina jednající v jeho zastoupení, nebo pachatel jedná sám za sebe. Pachatelé se skrývají pod různými IP adresami, které mohou být přesměrovaný přes různé země.

Čínská vláda chápe kybernetickou válku jako nástroj v boji proti americké moci a zároveň jako způsob získání asymetrické výhody proti mnohem silnějšímu protivníkovi. Strach, že druhá strana zasáhne první, vede k závodu ve zbrojení a militarizaci kyberprostoru. ČLR si uvědomuje roli kybernetické války a význam informací v současném informačním věku a je velmi aktivní v rozvíjení své vojenské strategie a doktríny pro vedení informačních vojenských operací, jejichž cílem je získání informační dominance nad protivníkem. Zároveň si uvědomuje zranitelnost USA, jíž je vysoká míra závislosti na informačních a komunikačních technologiích. Faktory, které eventuálně mohou vést k eskalaci konfliktu na kybernetické úrovni, jsou především čínská a americká vojenská strategie preferující první úder, minimální hranice pro zahájení útoku v této oblasti a vzájemná možná spojitost mezi kybernetickým a konvenčním válčením.

V rámci diplomové práce byla testována hypotéza, že mezi Čínou a Spojenými státy probíhá kybernetická válka. Konkrétním případem byl americko-čínský letecký incident z roku 2001, který se vyvinul v hackerskou válkou. Incident byl charakteristický tím, že představoval případ konfliktu, jehož příčinou byl fyzický střet (letecká havárie) s následky odehrávajícími se v kyberprostoru. Příčina leteckého incidentu nesouvisela s žádnými aktivitami v kyberprostoru. Tento případ nemůže být považován z hlediska státocentrické definice ani podle Tallinnského manuálu za příklad kybernetické války, neboť jednak nenaplnil podmínky ozbrojeného útoku a nezpůsobil fyzické škody, jednak se neodehrával mezi státy, nýbrž mezi nestátními aktéry. Útoky byly politicky motivované a vlastenecky zabarvené. Napadené stránky obsahovaly státní vlajky, politické slogany a fotografie pohřešovaného pilota. Politicky motivovaný hacking, představuje novou formu protestu, která se stává díky internetu mnohem účinnější, neboť poselství zainteresovaných skupin může prostřednictvím internetu oslovit širokou skupinu populace. Podle charakteristik konfliktu se jednalo o případ síťové války odehrávající se na společensko-ideové úrovni. Hypotéza byla tedy vyvrácena.

Případy kybernetických špionážních aktivit Číny proti americkým cílům má vážné dopady na vzájemné vztahy mezi oběma zeměmi. Úsilí Spojených států přimět Čínu k odpovědnosti za kybernetickou špionáž zůstává bez výraznější odezvy. Aféra ohledně Edwarda Snowdena navíc ztížila vyjednávací pozici Spojených států. Čína opakovaně odmítá

jakékoliv zapojení do kybernetické špionáže proti Spojeným státům a naopak nabádá k bilaterální a multilaterální spolupráci při sestavení pravidel v oblasti kybernetické bezpečnosti. Napomáhá jí také fakt, že mezinárodní právo nepovažuje špionáž za protizákonnou a charakter kyberprostoru umožňuje provádět aktivity přes různé IP adresy a pachatele lze jen stěží vypátrat a následné potrestání konkrétních viníků je rovněž těžko proveditelné, neboť jako tomu bylo v případě čínských vojáků, existuje nulová šance, že by byli vydáni pro soudní řízení a vykonání trestu. Americká vláda obstarala dostatek důkazů, aby potvrdila, že kybernetické útoky pocházely z území Číny, a dokonce byly prokazatelně podporované státem. Činy byly prováděné pod falešnou identitou a informace byly získány za účelem ekonomického prospěchu, neboť vyspělé technologie a vědecké poznatky představují hnací motor ekonomického rozvoje. Americká vláda se odhodlala k bezprecedentnímu kroku, kdy proti čínským armádním důstojníkům – hackerům vydala zatykač. Je to vůbec první případ obvinění jednotlivců, kteří podnikali nelegální kybernetické aktivity ve službách a z příkazu jiného státu.

Případ obviněného čínského podnikatele Su Bina představuje další případ kybernetické špionáže proti americkým společnostem. Na rozdíl od pěti vojenských důstojníků, Su Bin podle trestního oznámení pracoval pro své vlastní finanční obohacení. Spojení s čínskou vládou nebylo potvrzeno. Pachatel jednal sám za sebe, a tudíž se jednalo o kybernetický zločin. Dopadenému Su Binovi hrozí za vznesená obvinění trest odnětí svobody v maximální výši 30 let.

Vzhledem k prudkému rozvoji kybernetických aktivit – jak v oblasti civilní, tak vojenské – lze předpokládat, že počet případů mezinárodní kyber kriminality a špionáže bude i nadále narůstat. Absence mezinárodního režimu kybernetické bezpečnosti by měla zainteresované aktéry vést k mezinárodnímu dialogu a hledání všeobecně přijatelného řešení.

Použité zdroje

Elektronické zdroje

1. ABC. China leads the world in hacking. *ABC* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.abc.net.au/lateline/content/2014/s4009469.htm

2. ARQUILLA, J., RONFELDTSTR, D. Cyberwar is coming!. *RAND Corporation Syndicate* [online]. 1993 [cit. 2015-04-26]. Dostupné z: http://www.rand.org/pubs/reprints/RP223

3. BBC. Profile: Edward Snowden. *BBC* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.bbc.com/news/world-us-canada-22837100

4. Bezpečnostní informační služba. Terorismus. *Bezpečnostní informační služba* [online]. [cit. 2015-04-26]. Dostupné z: http://www.bis.cz/terorismus.html

5. BUCKLEY, Ch. Chinese Defense Ministry Accuses U.S. of Hypocrisy on Spying. *The New York Times* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.nytimes.com/2013/06/28/world/asia/chinese-defense-ministry-accuses-us-of-hypocrisy-on-spying.html

6. CARR Jeffrey. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, Inc. [online]. 2009 [cit. 2015-04-26]. Dostupné z: http://books.google.cz/books?id=5LIyXzpKhYsC&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

7. CCTV. Building networks to achieve power is an important part of Chinese Dream. *CCTV* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://opinion.cntv.cn/2014/02/27/ARTI1393510735234281.shtml

8. CNN.com. Feds warn of May Day attacks on U.S. Web sites. *CNN.com* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://edition.cnn.com/2001/TECH/internet/04/26/hacker.warning/index.html

9. College of Defence Studies, NDU, PLA, CHINA. National Defense Policy. *College of Defence Studies* [online]. [cit. 2015-04-26]. Dostupné z: http://www.cdsndu.org/html_en/to_xygk_orderNo=2701&superOrderNo=2700.html

10. CORNISH, P. On Cyber Warfare. *Chatham House* [online]. 2010 [cit. 2015-04-26]. Dostupné z: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf

11. Council of Europe. Convention on Cybercrime. *Council of Europe* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

12. Council of Europe. Convention on Cybercrime. *Council of Europe* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

13. CPC Central Committee and State Council. Opinions for Strengthening Information Security Assurance Work. *CPC Central Committee and State Council* [online]. 2003 [cit. 2015-04-26]. Dostupné z: http://wenku.baidu.com/view/7a967018227916888486d755.html

14. CRS Report for Congress. China-U.S. Aircraft Collision Incident of April, 2001: Assessments and Policy Implications. *CRS Report for Congress* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://fas.org/sgp/crs/row/RL30946.pdf

15. ČEJKA, M. Průvodce inteligentního čtenáře po arabském jaru. *iDNES.cz* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://zpravy.idnes.cz/vysla-zasadni-kniha-o-fenomenu-arabskeho-jara-fa2-/zpr_archiv.aspx?c=A120530_184151_kavarna_tul

16. DENNING, D. Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. *Georgetown University* [online]. 2000 [cit. 2015-04-26]. Dostupné z: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

17. Department of Defense. Department of Defense Strategy for Operating in Cyberspace, 2011

18. DOLEŽEL, M. NATO svazuje kyber-prostor. *Natoaktual.cz* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://www.natoaktual.cz/nato-svazuje-kyber-prostor-druha-cast-dxs-/na_analyzy.aspx?c=A111212_091109_na_analyzy_m02

19. DYER, G. a HILLE, K. US shrugs off Snowden leaks to press Beijing on cyber theft. *Financial Times* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.ft.com/intl/cms/s/0/6ed4960a-e6f6-11e2-aa48-00144feabdc0.html

20. European Comission. What is cybercrime?. *European Comission* [online]. 2015 [cit. 2015-04-26]. Dostupné z: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

21. FEAKIN, T. ARF, and how to change the tune of the cyber debate. *Australian Strategic Policy Institute* [online]. 2013 [cit. 2015-04-26]. Dostupné z: *http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/*

22. Federation of American Scientists. Foreign Intelligence Surveillance Act. *FAS* [online]. 2015 [cit. 2015-04-26]. Dostupné z: http://fas.org/irp/agency/doj/fisa/

23. Financial Times. Definition of industrial espionage. *Financial Times* [online]. [cit. 2015-04-26]. Dostupné z: *http://lexicon.ft.com/Term?term=industrial-espionage*

24. FUČÍK, J., KŘÍŽ, Z. Informační revoluce, vojensko-technická revoluce, nebo revoluce ve vojenských záležitostech?. *Obrana a strategie* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.obranaastrategie.cz/en/archive/volume-2013/2-2013/articles/information-revolution-military-technical-revolution-or-revolution-in-military-affairs.html#.VSJzIzvkfgU

25. GEERS, K. Cyberspace and the Changing Nature of Warfare. *U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia* [online]. 2008 [cit. 2015-04-26]. Dostupné z: http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf

26. Georgetown Security Studies Review. Richard A. Clarke and Robert K. Knake's "Cyber War: The Next Threat to National Security and What to Do About It". *Georgetown Security Studies Review* [online]. 2010 [cit. 2015-04-26]. Dostupné z:

http://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/

27. GOMPERT, D. a LIBICKI, M. Cyber Warfare and Sino-American Crisis Instability. *Survival: Global Politics and Strategy August–September 2014* [online]. 2014 [cit. 2015-04-26]. Dostupné z: https://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc

28. GREENWALD, G. a MACASKILL, E. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

29. GROSSMAN, A. a YADRON, D. U.S. Accuses Chinese Executive of Hacking to Mine Military Data. *The Wall Street Journal* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.wsj.com/articles/u-s-accuses-chinese-executive-of-hacking-to-find-military-data-1405105264

30. HSU, K. China and International Law in Cyberspace. *U.S.-China Economic and Security Review Commission* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

31. CHANG, A. Warring State: China`s Cybersecurity Strategy. *Center for a New American Security* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf

32. China Daily.com.cn. Full Text: White paper on the Internet in China. *China Daily.com.cn* [online]. 2010 [cit. 2015-04-26]. Dostupné z: http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_6.htm

33. Institute on Global Conflict and Cooperation. China and Cybersecurity: Political, Economic, and Strategic Dimensions. *Institute on Global Conflict and Cooperation* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://igcc.ucsd.edu/assets/001/503568.pdf

34. Internet Live Stats. Internet Users by Country (2014). *Internet Live Stats* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.internetlivestats.com/internet-users-by-country/

35. Internet World Stats. World Internet Users and 2014 Population Stats. *Internet World Stats* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.internetworldstats.com/stats.htm

36. ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity. *ISO* [online]. 2012 [cit. 2015-04-26]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en

37. ITU. Definition of cybersecurity. *ITU* [online]. © ITU 2015 [cit. 2015-04-26]. Dostupné z: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

38. ITU. Definition of cybersecurity. *ITU* [online]. 2015 [cit. 2015-04-26]. Dostupné z: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

39. KLIMBURG, A. (ed.). National Cyber Security Manual, NATO CCD COE Publication, Tallinn [online]. 2012 [cit. 2015-04-26]. Dostupné z: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

40. KRAMER, F. a STARR, S. Cyberpower and National Security. *Potomac Books, Inc.* [online]. 2009 [cit. 2015-04-26]. Dostupné z: https://www.google.cz/books?id=cj8FUPKipzAC&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

41. KUEHL D. From Cyberspace to Cyberpower. Defining the Problem. [online]. 2009 [cit. 2015-04-26]. Dostupné z: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf

42. LAM, L. Edward Snowden: US government has been hacking Hong Kong and China for years. *South China Morning Post* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china?page=all

43. LÁZŇOVSKÝ, M. a KASÍK, P. Zprávu o sledování lidí na internetu vynesl bývalý technik CIA. Utekl z USA. *Technnet.cz* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://technet.idnes.cz/unik-informaci-z-nsa-ma-na-svedomi-edward-snowden-f6r-/sw_internet.aspx?c=A130609_212955_sw_internet_brm

44. LEWIS, A. a HANSEN, S. China's cyberpower: International and domestic priorities. *Australian Strategic Policy Institute* [online]. 2014 [cit. 2015-04-26]. Dostupné z: https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf

45. LIEW, L. a VANG, S. Nationalism, Democracy and National Integration in China. *Routledge* [online]. 2012 [cit. 2015-04-26]. Dostupné z: *https://books.google.cz/books?id=9gJVvOEzqrQC&pg=PT192&lpg=PT192&dq=chinese+public+opinion+hainan+incident&source=bl&ots=NxvprFjjsQ&sig=5_iZncfNtIyNLfrexpaDq5zGO3c&hl=cs&sa=X&ei=OrQWVb2VOMPvatLwgogG&ved=0CCUQ6AEwAA#v=onepage&q=chinese%20public%20opinion%20hainan%20incident&f=false*

46. MACKINNON, R a MOROZOV, E. Firewalls to Freedom. *Project Syndicate* [online]. 2009 [cit. 2015-04-26]. Dostupné z: *http://www.project-syndicate.org/commentary/firewalls-to-freedom*

47. MANDIANT. APT1: Exposing One of China's Cyber Espionage Units. *Mandiant* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://intelreport.mandiant.com/

48. MCGREGOR, R. Obama and Xi talks tackle cyber security. *Financial Times* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.ft.com/intl/cms/s/0/ee0612aa-d094-11e2-be7b-00144feab7de.html

49. MCMAHON, R. U.S. Internet Providers and the 'Great Firewall of China'. *Council on Foreign Relations* [online]. 2011 [cit. 2015-04-26]. Dostupné z: http://www.cfr.org/internet-policy/us-internet-providers-great-firewall-china/p9856

50. Ministerstvo průmyslu a obchodu. *Výsledek Světové konference o mezinárodních telekomunikacích. Ministerstvo průmyslu a obchodu* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://www.mpo.cz/dokument118663.html

51. Ministerstvo vnitra České republiky. Základní definice, vztahující se k tématu kybernetické bezpecnosti. *Ministerstvo vnitra České republiky* [online]. 2009 [cit. 2015-04-26]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

52. Ministry of Foreign Affairs of the People`s Republic of China. China strongly attacks the United States "to prosecute" Chinese officials. *Ministry of Foreign Affairs of the People`s Republic of China* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.mfa.gov.cn/mfa_chn/fyrbt_602243/t1157478.shtml

53. Ministry of National Defense of the People`s Republic of China. Defense Ministry spokesman Geng Yansheng's Remarks on the US Justice Department to prosecute Chinese soldiers. *Ministry of National Defense of the People`s Republic of China* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://news.mod.gov.cn/headlines/2014-05/20/content_4510313.htm

54. NATO Cooperative Cyber Defence Centre of Excellence. Tallin Manual Process. *CCDCOE* [online]. [cit. 2015-04-26]. Dostupné z: https://ccdcoe.org/research.html

55. NYE, J. Is Military Power Becoming Obsolete*?, Project Syndicate* [online]. 2010 [cit. 2015-04-26]. Dostupné z: http://www.project-syndicate.org/commentary/is-military-power-becoming-obsolete

56. NYE, J. The Information Revolution Gets Political. *Project Syndicate* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.project-syndicate.org/commentary/information-technology-s-political-implications-by-joseph-s--nye/czech

57. OECD. Glossary of Statistical Terms. Digital divide. *OECD* [online]. 2002 [cit. 2015-04-26]. Dostupné z: https://stats.oecd.org/glossary/detail.asp?ID=4719

58. OECD. Recommendation of the Council on the Protection of Critical Information Infrastructures*, OECD* [online]. 2008 [cit. 2015-04-26]. Dostupné z: http://www.oecd.org/sti/40825404.pdf

59. Office of the Director of National Intelligence. DNI Statement on Activities Authorized Under Section 702 of FISA, *Office of the Director of National Intelligence*

[online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa

60. Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012. *Office of the Secretary Defense* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf

61. Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013. *Office of the Secretary Defense* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf

62. OTTIS, R., LORENTS, P. Cyberspace: Definition and Implications. *Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf

63. People`s Daily. Domineering Action and Hegemonic Logic. *People`s Daily* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://fas.org/news/china/2001/china-010405.htm

64. SANGER, D. - BARBOZA, D. – PERLROTH, N. Chinese Army Unit Is Seen as Tied to Hacking Against U.S. *The New York Times* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

65. SANGER, D. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

66. SHACKELFORD, S. Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance. *American University Law Review House* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1888&context=aulr

67. SCHMITT M. (ed.). Tallinn Manual on Interneational Law Applicable to Cyber Warfare. Cambridge University Press. [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

68. SINGER, P. a FRIEDMAN, A. Cybersecurity and Cyberwar: What everyone need to know. *Oxford University Press* [online]. 2014 [cit. 2015-04-26]. Dostupné z: https://www.google.cz/books?hl=cs&lr=&id=9VDSAQAAQBAJ&oi=fnd&pg=PP2&dq=SINGER,+P.+Cybersecurity+and+Cyberwar:+what&ots=80jMS5xLZd&sig=Wxf-I9dUn4ZXkAKMKeNl3Mvpndc&redir_esc=y#v=onepage&q=SINGER%2C%20P.%20Cybersecurity%20and%20Cyberwar%3A%20what&f=false

69. SMITH, C. May 6-12; The First World Hacker War. *The New York Times.* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html

70. SWAINE, M. Chinese Views on Cybersecurity in Foreign Relations. *Carnegie Endowment for International Peace* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf

71. TANG, R. China-U.S. cyber war escalates. *CNN.com* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/index.html

72. The Central People`s Government of the People`s Republic of China. State Council Opinion on Vigorously Promoting the Development of Informatization and Effective Protection of Information Security. *The Central People`s Government of the People`s Republic of China* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm

73. The Embassy of PRC in New Zealand. *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*. *The Embassy of PRC* [online]. 2011 [cit. 2015-04-26]. Dostupné z: http://nz.chineseembassy.org/eng/zgyw/t858978.htm

74. The FBI. Cyber's Most Wanted. *The FBI* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.fbi.gov/wanted/cyber

75. The FBI. Los Angeles Grand Jury Indicts Chinese National In Computer Hacking Scheme Allegedly Involving Theft Of Trade Secrets. *U.S. Attorney's Office* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.fbi.gov/losangeles/press-releases/2014/los-angeles-grand-jury-indicts-chinese-national-in-computer-hacking-scheme-allegedly-involving-theft-of-trade-secrets

76. The FBI. U.*S.* Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. *U.S. Department of Justice* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage

77. The Information Warfare Site. "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May". *The Information Warfare Site* [online]. 2001 [cit. 2015-04-26]. Dostupné z: http://www.iwar.org.uk/infocon/advisories/2001/01-009.htm

78. *The North Atlantic Treaty* (1949), Washington D.C.

79. The White House. Executive Order -- Improving Critical Infrastructure Cybersecurity. *The White House* [online]. 2013 [cit. 2015-04-26]. Dostupné z: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

80. The White House. *Foreign Policy, Cybersecurity. The White House* [online]. [cit. 2015-04-26]. Dostupné z: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

81. The White House. International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World. *The White House* [online]. 2011 [cit. 2015-04-26]. Dostupné z: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

82. The White House. National Security Stratety, 2010

83. The White House. National Strategy for Information Sharing and Safeguarding, 2012

84. TIEZZI, S. China's 'Sovereign Internet'. *The Diplomat* [online]. 2014 [cit. 2015-04-26]. Dostupné z: *http://thediplomat.com/2014/06/chinas-sovereign-internet/*

85. TIEZZI, S. The New US Court Case Against Chinese Hacking. *The Diplomat* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://thediplomat.com/2014/07/the-new-us-court-case-against-chinese-hacking/

86. TIKK, E. Ten Rules for Cyber Security. *Survival: Global Politics and Strategy* [online]. 2011 [cit. 2015-04-26]. Dostupné z: http://www.jgu.edu.in/joss/PDF/TenRulesforCyberSecuritySurvival.pdf

87. U.S.-China Economic and Security Review Commission. 2013 Report to Congress of the U.S.-China Economic and Security Review Commission. *U.S. Government Printing* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://origin.www.uscc.gov/sites/default/files/annual_reports/Complete%202013%20Annual%20Report.PDF

88. UK Cabinet Office, Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. *UK Office of Cyber Security* [online]. 2009 [cit. 2015-04-26]. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

89. UN General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN General Assembly* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.mofa.go.jp/files/000016407.pdf

90. UN General Assembly. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council* [online]. 2011 [cit. 2015-04-26]. Dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

91. UN General Assembly. Universal Declaration of Human Rights. *United Nations* [online]. 1948 [cit. 2015-04-26]. Dostupné z: http://www.refworld.org/docid/3ae6b3712c.html

92. UNODA. Developments in the Fields of Information and Telecommunications in the context of International Security. *UNODA* [online]. 2010 [cit. 2015-04-26]. Dostupné z: http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf

93. WAISOVÁ, Š. Od národní bezpečnosti k mezinárodní bezpečnosti. Kodaňská škola na křižovatce strukturálního realismu, anglické školy a sociálního konstruktivismu. *Mezinárodní vztahy* [online]. 2004 [cit. 2015-04-26]. Dostupné z: https://mv.iir.cz/article/download/124/pdf

94. WASUO, H. B. Information Space, 2000. *In*: GILES, K. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. *NATO CCD COE Publications, Tallinn* [online]. 2013 [cit. 2015-04-26]. Dostupné z: https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

95. WORTZEL, L. The Chinese People`s Liberation Army and Information Warfare. *The Strategic Studies Institute* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1191.pdf

96. YU, M. Party Directs China`s Twitter. *The Washington Times* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://www.washingtontimes.com/news/2012/feb/8/inside-china-719761130/?page=all

97. ZHAO, S. Chinese Pragmatic Nationalism and Its Foreign Policy Implications. *Graduate School of International Studies University of Denver* [online]. 2008 [cit. 2015-04-26]. Dostupné z: http://www.lsu.edu/artsci/groups/voegelin/society/2008%20Papers/Suisheng%20Zhao.pdf

Knižní monografie

98. BUZAN, B., WAEVER, O. a WILDE, J. Bezpečnost: nový rámec pro analýzu. 1. vyd. Brno: Centrum strategických studií, 2005, 267 s. Současná teorie mezinárodních vztahů. ISBN 80-903333-6-2.

99. FIŘTOVÁ, M. (ed.) a KOZÁK, K. (ed.). Spojené státy v úpadku?: vybrané problémy veřejné politiky v severoamerickém kontextu. 1. vyd. Praha: Dokořán, 2013. 287 s. Bod. ISBN 978-80-7363-545-9.

100. JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

101. LEHMANNOVÁ, Zuzana. Formování globálního řádu?: globalizace a global governance. Vyd. 1. V Praze: Oeconomica, 2010, 287 s. ISBN 978-80-245-1649-3.

102. NYE, J. The future of power. 1st ed. New York: PublicAffairs, 2011, xviii, 298 s. ISBN 9781610390699.