UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií

Barbora Debnárová

Kybernetická bezpečnost: vztah USA a Číny

Diplomová práce

Praha 2015

Autor práce: **Barbora Debnárová**

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

Rok obhajoby: **2015**

Bibliografický záznam

DEBNÁROVÁ, Barbora. *Kybernetická bezpečnost: vztah USA a Číny*. Praha, 2015. 71 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut politologických studií. Katedra mezinárodních vztahů. Vedoucí diplomové práce PhDr. Vít Střítecký, M.Phil., Ph.D.

Abstrakt

Předkládaná diplomová práce se zabývá kybernetickou bezpečností, konkrétně vztahem Spojených států amerických a Čínské lidové republiky v této oblasti.

Cílem této práce je odpovědět na následující otázky:

Jakou kybernetickou hrozbu představuje Čína pro Spojené státy americké? Jaká je čínská kybernetická strategie? Jak na tuto hrozbu reagují Spojené státy a jaké jsou mezery v jejich reakci?

Práce je rozdělena do čtyř kapitol. První kapitola se zabývá definicí *"cyberwarfare"* a jeho pojetím v čínském kontextu. Druhá kapitola řeší vztah USA a Číny a jeho dopad na kybernetickou bezpečnost. Třetí kapitola analyzuje reakci USA na čínskou kybernetickou hrozbu. Poslední kapitola představuje mezery v této strategii.

Abstract

This diploma thesis deals with cyber relation of the United States of America and the People´s republic of China.

The aim of this diploma thesis is to answer the following questions:

What kind of cyber threat for the United States does China represent? How is China´s cyber strategy characterised? How do USA react on this threat and what are the gaps in this reaction?

The thesis is divided into four chapters. The first chapter deals with definition of cyberwarfare and its perception in Chinese context. The second chapter analyses USA – China relation and its implication for cyber security. The third chapter represents US reaction on Chinese cyber threat. The last chapter deals with the gaps in the reaction.

Klíčová slova

USA, Čína, kybernetická hrozba, "*cyberwarfare"*, kybernetická špionáž

Keywords

USA, China, cyberthreat, cyberwarfare, cyber espionage

Rozsah práce

109 890 znaků

Prohlášení

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

V Praze dne 12.5.2015 Barbora Debnárová

Poděkování

Děkuji panu PhDr. Vítu Stříteckému, M.Phil., Ph.D. za jeho odborný dohled, trpělivost, pomoc a cenné připomínky při zpracování mé diplomové práce.

Obsah

Zoznam skratiek

APEC	*Asia-Pacific Economic Cooperation*
APT	*Advanced Persistent Threat*
ARFORCYBER	*Army Forces Cyber Command*
CNA	*Computer-Network Attack*
CNE	*Computer-Network Exploitation*
CND	*Computer-Network Defense*
CNO	*Computer-Network Operations*
DOD	*Department of Defense*
FBI	*Federal Investigation Bureau*
FLTCYBERCOM	*Fleet Cyber Command*
MARFORCYBER	*Marine Forces Cyber Command*
NSA	*National Security Agency*
NIPRNET	*Non-classified Internet Protocol Router Network*
PLA	*People´s Liberation Army*
PRC	*People´s Republic of China*
USCYBERCOM resp. CYBERCOM	*U.S. Cyber Command*

Zoznam tabuliek a obrázkov

Úvod

Obidve krajiny, USA i Čína, zastávajú významné role v oblasti svetovej politiky. Dokonca je možné zhodnotiť, že ich vzájomný vzťah je jedným z najdôležitejších vzťahov medzi štátmi - v súčasnosti a aj do budúcnosti. Oba totiž majú veľmi významné postavenie v mnohých kritických globálnych záležitostiach, ako je mier a bezpečnosť, obchod, financie či životné prostredie. Z uvedeného teda vyplýva, že to, ako s týmto vzťahom naložia, neovplyvní len ich vlastnú budúcnosť, ale aj budúcnosť celého sveta.

Tento ich vzájomný vzťah je už však od vytvorenia Čínskej ľudovej republiky v roku 1949 komplikovaný a poznačený vzájomnou nedôverou. V rámci všetkých problematických záležitostí, kybernetická bezpečnosť je tou, ktorá vytvorila najväčší rozruch v najkratšom čase. Tak krátky časový interval sa dá jednoducho vysvetliť technickým rozvojom a enormným nárastom v používaní informačných technológií za posledné roky.[1]

Dôležitým faktom však ostáva ohromná závislosť USA na informačných technológiách. Spojené štáty sa po studenej vojne stali neporaziteľnou mocnosťou v oblasti konvenčnej aj jadrovej sily. Avšak, ich vojenská neporaziteľnosť a vedúca pozícia v oblasti informačných technológií z nich takisto urobila krajinu najzraniteľnejšiu kybernetickým útokom. Nepriateľ je si v tomto prípade vedomý, že vo vojenskej oblasti nedokáže uspieť, a tak hľadá alternatívne metódy útoku. Kybernetický priestor sa v dnešnej dobe stal priestorom ideálnym pre tieto typy útokov. Závislosť USA na informačných technológiách sa teda môže stať Achillovou pätou tohto zdanlivo neohroziteľného štátu.[2]

Čínska ľudová republika naopak zastáva prominentnú pozíciu medzi krajinami prevádzajúcimi kybernetické útoky na iné štáty. Jej hlavným cieľom je Taiwan, no často sú napádané aj inštitúcie iných zemí, predovšetkým noviny, ministerstvá, ambasády, vládne a nevládne organizácie. Faktom je, že Číňania už od roku 1991 vyvíjajú a dosadzujú pokročilé technológie do ich vlády, vojenského a civilného sektoru v rámci úsilia o vybudovanie čínskej hospodárskej a politickej sily. Okrem toho je toto považované za úsilie o vytvorenie protiváhy

[1] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[2] ADAMS, James. Virtual Defense: THE WEAKNESS OF A SUPERPOWER. *Foreign Affairs* [online]. 2001, May/June 2001 [cit. 2014-05-18]. Dostupné z: http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

k americkej vojenskej nadradenosti. Ba čo viac, Čína uznáva kybernetický priestor ako bojovú doménu a kybernetickú moc dáva do jednej roviny s pozemskou, vodnou a vzdušnou vojenskou silou.[3]

Za posledné roky bolo zaznamenaných niekoľko kybernetických útokov na vládu, armádu či kritickú infraštruktúru Spojených štátov, ktoré zapadajú do konceptu *„cyberwarfare“*, a za ktoré je obviňovaná Čína. V súčasnosti je však väčšia pozornosť venovaná ekonomickej kybernetickej špionáži. Správa vydaná *„United States-China Economic and Security Review Commission“*[4] z roku 2014 s názvom *„2014 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION“* uvádza, že čínska vláda od polovice roku 2000 prevádzkuje široko – škálovú špionáž proti Spojeným štátom. Hodnota ukradnutých dát dosiahla výšku 338 miliárd dolárov ročne.[5] Mnohé z týchto útokov dokonca vykazujú spojitosť medzi *„cyberwarfare“* a ekonomickou špionážou, čo je pre túto prácu veľmi dôležité.

V mojej diplomovej práci budem totiž vychádzať zo skutočnosti, že všeobecná definícia *„cyberwarfare“* v prípade Číny nie je úplne platná. Zvláštnym spôsobom je tam totižto premiešaný vojenský a súkromný sektor, *„cyberwarfare“* a ekonomická špionáž. Čínska armáda v súlade so svojou doktrínou[6] *„cyberwarfare“* na výkon svojich vojenských kybernetických operácií používa zamestnancov z akademickej pôdy a informačne technologického priemyslu a civilných hackerov.[7] Obranná politika Číny sa snaží o koordinovaný vývoj hospodárstva a národnej obrany, a tak Čína kybernetické útoky využíva s dvojakým cieľom – na podporu armády aj ekonomiky. Väčšina čínskej kybernetickej hospodárskej špionáže mieri na americké komerčné ciele, ktorých činnosť sa nejako spája

[3] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[4] United States-China Economic and Security Review Commission je kongresovou skupinou Vlády Spojených štátov. Bola založená v roku 2000 s cieľom monitorovania národne bezpečnostných a obchodných záležitostí medzi USA a Čínou. Okrem iných aktivít, každoročne vydáva svoju správu.

[5] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[6] MAZANEC, Brian M. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

[7] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

s vojenskou technológiou.[8] Na základe týchto faktov budem v práci predpokladať, že čínsku vojenskú a ekonomickú kybernetickú hrozbu pre USA od seba nie je možné celkom oddeliť.

Práca sa trochu odchyľuje od schváleného výskumného projektu. Došlo k tomu po konzultáciách s vedúcim práce a jedná sa viac menej o špecifikáciu problematiky.

Cieľom mojej diplomovej práce je zodpovedať na nasledujúce otázky. Akú kybernetickú hrozbu predstavuje Čína pre Spojené štáty americké? Ako má nadefinovanú svoju kybernetickú stratégiu? Ako na túto hrozbu reagujú USA a aké sú medzery v ich reakcii?

V práci budem pracovať s originálnym anglickým pojmom *„cyberwarfare"*, a to kvôli neschopnosti nájsť adekvátny slovenský preklad. Preklad kybernetická vojna nepovažujem úplne za správny. Podľa definície, s ktorou vo svojom článku pracuje tiež Jayson Spade,[9] kybernetickú vojnu považujem za konflikt, v rámci ktorého sa bojuje výlučne v kybernetickom priestore a sú pri ňom používané iba počítače a to za účelom útoku na siete protivníka. *„Cyberwarfare"* vnímam ako súčasť väčšieho, tradičného konfliktu používanú spoločne s inými prostriedkami národnej sily, ktorej cieľom je zničenie alebo degradácia protivníkových sietí za účelom ovplyvnenia celého priebehu konfliktu.[10] Za relevantnejší preklad do slovenčiny by som považovala termín *„kybernetické vedenie vojny"*, no predsa radšej uprednostním zostať pri anglickom originály. Názvy inštitúcií, dokumentov a niektoré technické pojmy tiež ponechám v angličtine.

Použitou metodológiou je prípadová štúdia americko – čínskeho kybernetického vzťahu.

Diplomová práce bude rozčlenená do štyroch kapitol.

V prvej, teoretickej kapitole práce sa budem venovať pojmu *„cyberwarfare"* všeobecne, a tiež v kontexte Čínskej ľudovej republiky. Zameriam sa predovšetkým na rozdiel medzi všeobecnou definíciou *„cyberwarfare"* a spôsobom, akým ho definujú Číňania.

V druhej kapitole sa budem zaoberať kybernetickou hrozbou Číny pre bezpečnosť Spojených štátov amerických. Na začiatku kapitoly popíšem medzinárodný význam týchto štátov a ich vzájomný vzťah za účelom naznačenia dôvodov, prečo majú tieto krajiny jedna o druhú

[8] Ibid
[9] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf
[10] Ibid

záujem, medziiným aj v kybernetickej oblasti. Pokračovať budem kybernetickou hrozbou Číny pre USA, ktorú rozdelím na dve kategórie: vojenská a ekonomická.

V tretej kapitole budem riešiť to, akým spôsobom sa Spojené štáty bránia proti čínskej vojenskej a ekonomickej kybernetickej hrozbe. Vo vojenskej sa budem venovať vzniku nových inštitúcií a strategických dokumentov, v ekonomickej budem riešiť obviňovanie Číny z kybernetických útokov zo strany USA, vzájomný dialóg a spoluprácu v kybernetickej oblasti, ekonomické sankcie a opatrenia prijaté vo vnútri Spojených štátov.

V štvrtej kapitole identifikujem medzery v jednotlivých spôsoboch, ktorými sa USA proti čínskej kybernetickej hrozbe bráni a nezrovnalosti v stratégii USA.

Čo sa týka literatúry, z ktorej budem čerpať, vo svojej diplomovej práci budem pracovať s odbornými knihami, článkami z odborných časopisov a primárnymi dokumentmi v podobe stratégií, správ či záznamov stretnutí, pričom prevažnú časť tvoria články a primárne zdroje.

Z knižných zdrojov boli pre mňa dôležité tituly *„American images of China: identity, power, policy“* od Olivera Turnera, *„China, the United States, and global order“* od Rosemary Foot a Andrewa Waltera, *„China among unequals: asymmetric foreign relationships in Asia“* od Brantlyho Womacka a *„Spojené štáty v úpadku“* od Magdaleny Fiřtovej a Kryštofa Kozáka, ktoré budú použité predovšetkým v kapitole zaoberajúcej sa vzájomným vzťahom USA a Číny.

Oliver sa Turner vo svojej knihe *„American images of China: identity, power, policy“* zaoberá vzťahom USA a Číny od roku 1949. Brantly Womack v *„China among unequals: asymmetric foreign relationships in Asia“* predstavuje nové paradigma štúdia medzinárodných vzťahov nazvané teória asymetrie, odvodené zo vzťahov Číny s okolitými štátmi a zvyškom sveta. Foot a Walter sa v *„China, the United States, and global order“* venujú rôznym dimenziám čínsko – amerického vzťahu od roku 1945. Magdaléna Fiřtová a Kryštof Kozák sa v *„Spojené štáty v úpadku“* zaoberajú hrozbou, ktorú Čína potenciálne predstavuje pre postavenie USA ako svetovej superveľmoci.

Vo všeobecnej teoretickej časti budú pre mňa za účelom definície pojmu *„cyber warfare“* významné články *„Principles of Cyber-warfare“* od Raymonda C. Parksa a Davida P. Duggana, *„On Cyberwarfare“* od Freda Schreiera a *„Apocalyptic Visions: Cyber War and the Politics of Time“* od Tima Stevensa.

V teoretickej časti o čínskom *„cyberwarfare“* budú pre mňa užitočné články *„China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence“* od Magnusa Hjortdala, *„China´s cyber power and America´s national security“* od Jaysona M. Spada, *„The Art of Cyber War“* od Briana M. Mazanca, *„Information Warfare: An Emerging and Preferred Tool of the People's Republic of China“* od Gerryho M. Perry, *„On Cybersecurity The Impact of China on Cybersecurity“* od Jona R. Lindsaya a *„Chinese Views on Cybersecurity in Foreign Relations“* od Michaela D. Swaine. Perry a Hjortdal vo svojich článkoch riešia hlavne čínsku doktrínu *„cyberwarfare“*. Mazanec, Spade, Swaine a Lindsay sa zaoberajú čínskymi kybernetickými kapacitami v oblasti *„cyberwarfare“*.

V práci budem tiež často pracovať s primárnymi zdrojmi, ktoré pre mňa budú dôležité hlavne pri identifikácii čínskej kybernetickej hrozby pre bezpečnosť USA, spôsobov, akými sa USA bránia a medzier v ich stratégii. Medzi najvýznamnejšie z nich určite patria správy od organizácie Mandiant *„The Advanced Persistent Threat“* z roku 2010 a „APT1: Exposing One of China's Cyber Espionage Unit“ z roku 2013 zaoberajúce sa takzvanými „Advanced Persistent Threat (APT)“, tímami venujúcimi sa kybernetickou špionážou, ktoré majú byť údajne sponzorované čínskou vládou. Ďalšími sú strategické dokumenty americkej vlády, konkrétne *„Department of Defense Cyber Strategy“* a *„National Security Strategy“* z roku 2015. V snahe o identifikáciu aktuálnych problémov medzi USA a Čínou v oblasti kybernetickej bezpečnosti a tiež iných bezpečnostných a hospodárskych oblastiach bude ťažiskovým dokumentom *„REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION“* z roku 2014. Značne tiež budem čerpať zo záznamu z debaty pri okrúhlom stole v *„UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION“* nazvanej *„U.S.-CHINA CYBERSECURITY ISSUES“* z roku 2013.

1. Teoretická časť

1.1. Cyberwarfare

1.1.1. Definícia

V priebehu posledných dvoch dekád sa kybernetický priestor a kybernetická sila stali vo vojenskej oblasti veľmi významnými nástrojmi tvoriacimi jadro mnohých vojenských konceptov a doktrín.[11] S pojmom kybernetický priestor sa úzko viaže pojem *„cyberwarfare“*, pre ktorý dodnes neexistuje univerzálne akceptovaná definícia.[12] Uvediem ich teda niekoľko.

Vo všeobecnosti je názvom *„cyberwarfare“* označovaný masívne koordinovaný digitálny útok na nejakú vládu realizovaný inou vládou alebo väčšou skupinou obyvateľstva za účelom vniknutia do jej sietí, spôsobujúc ich poškodenie alebo zničenie. Podľa tejto definície však *„cyberwarfare“* môžeme nazývať aj útoky medzi spoločnosťami, teroristickými organizáciami alebo hackermi, ktoré sa zdajú byť podobné vojne.[13]

Tim Stevens vo svojom článku *„Apocalyptic Visions: Cyber War and the Politics of Time“* charakterizuje *„cyberwarfare“* ako taktické použitie informácií a informačných sieťových technológií štátnymi ozbrojenými silami.[14]

Raymond C. Parks a David P. Duggan ho zasa vo svojom článku *„Principles of Cyber-warfare“* definujú ako podmnožinu *„information warfare“*, ktorá sa odohráva v kybernetickom priestore, pričom za kybernetický priestor považujú akúkoľvek virtuálnu realitu nachádzajú sa v spojení počítačov a sietí. Kybernetických priestorov je podľa nich mnoho, no najvýznamnejším pre *„cyberwarfare“* je internet.[15]

---

[11] SCHREIER, Fred. On Cyberwarfare. [online]. 2015, s. 133 [cit. 2015-04-25]. Dostupné z: www.dcaf.ch/.../file/OnCyberwarfare-Schreier.pdf

[12] Ibid

[13] Ibid

[14] STEVENS, Tim. Apocalyptic Visions: Cyber War and the Politics of Time. *Social Science Research Network* [online]. 2013, s. 28 [cit. 2015-04-25]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2256370

[15] PARKS, Raymond C. Parks and David P. Duggan a David P. DUGGAN. Principles of Cyber-warfare. [online]. 2001 [cit. 2015-04-25]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf

Iná definícia, ktorú vo svojom článku použil Fred Schreier, ho charakterizuje ako asymetrickú alebo symetrickú, ofenzívnu alebo defenzívnu, digitálnu sieťovú aktivitu vykonávanú aktérmi štátneho charakteru predstavujúcu nebezpečenstvo pre národnú kritickú infraštruktúru a vojenský systém, ktorá vyžaduje vysoký stupeň vzájomnej závislosti medzi digitálnymi sieťami a infraštruktúrou na strane napadnutého a technologickou nadradenosťou na strane útočníka, a ktorá má byť chápaná viac v kontexte budúcej než prítomnej hrozby.[16]

Generálny a výkonný riaditeľ Londýnskeho *„International Institute for Strategic Studies“*, John Chipman, o ňom povedal nasledovné: *„... budúce medzištátne konflikty môžu byť charakterizované použitím takzvaných asymetrických techník. Vedúcou medzi nimi môže byť „cyberwarfare“*.[17]

Jayson M. Spade píše, že *„cyberwarfare“* je súčasťou väčšieho tradičného konfliktu a je používaný spolu s kombináciou pozemskej, námornej, vzdušnej, vesmírnej a ďalšími druhmi národnej sily. Pre útočníka, ktorý *„cyberwarfare“* používa, je cieľom zničenie alebo degradácia protivníkových informačných sietí a technológií so zámerom ovplyvniť celý priebeh konfliktu. Pre toho, ktorý sa bráni, je cieľom ochrániť svoje siete pred kybernetickým útokom.[18]

1.1.2. Koncepty cyberwarfare

V rámci NATO sa v súvislosti s *„cyberwarfare“* používa všeobecný termín *„Computer-Network Operations (CNO)“*. Tento sa skladá z troch prvkov. Prvým z nich je *„Computer-Network Exploitation (CNE)“* zahŕňajúci pokusy o získanie informácií o systéme, ktoré môžu byť použité pre budúce útoky. Druhým je *„Computer-Network Attack (CNA)“*, ktorý pokrýva pokusy o útoky na systémy. Tretím prvkom je *„Computer-Network Defense (CND)“*

[16] SCHREIER, Fred. On Cyberwarfare. [online]. 2015, s. 133 [cit. 2015-04-25]. Dostupné z: www.dcaf.ch/.../file/OnCyberwarfare-Schreier.pdf

[17] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[18] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

zahŕňajúci vlastnú obranu pred útokom. Efektívne CNA nemôže byť realizované bez súčasnej realizácie CNE a CND a naopak.[19]

1.1.3. Cyberwarfare v praxi

Úspešnosť aplikácie *„cyberwarfare"* závisí na použitých prostriedkoch a zraniteľnosti. Prostriedky reprezentujú nástroje, ľudí a kybernetické zbrane, ktoré má útočník k dispozícii. Zraniteľnosťou rozumieme rozsah všeobecnej závislosti hospodárstva a vojska nepriateľa na internete a sieťach.[20]

Asi najznámejším príkladom použitia *„cyberwarfare"* je vojenský kybernetický útok Ruska na Gruzínsko v roku 2008,[21] kedy boli napadnuté webové stránky a servery gruzínskej vlády, čím ju Rusi oslabili v kritickej fáze konfliktu.[22] Dodnes sa ešte presne nepodarilo určiť, kto za týmto útokom stojí.[23] Ďalším známym prípadom je útok Ruska na Estónsko z roku 2007. Tento útok mal za následok spomalenie estónskych vládnych sietí, respektíve ich prepnutie do offline režimu na dobu dvoch dní a ich následný reštart. Problémy vznikli aj pri používaní bankomatov a elektronického bankovníctva. Rusi tento útok mali spáchať z pomsty za prenesenie ruského vojenského pamätníka z Talinu.[24] Preslávený je tiež červ *„Stuxnet"*, ktorý mali USA vytvoriť v spolupráci s Izraelom a mal byť použitý na sabotáž iránskeho jadrového programu. V rámci operácie s názvom *„Olympijské hry"* boli realizované kybernetické útoky na zariadenia slúžiace na obohacovanie uránu v Natanze, ktoré na nich spôsobili závažné škody.[25] Z aktuálnejších prípadov stojí za zmienenie *„Duqu"* z roku 2011.

---

[19] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[20] SCHREIER, Fred. On Cyberwarfare. [online]. 2015, s. 133 [cit. 2015-04-25]. Dostupné z: www.dcaf.ch/.../file/OnCyberwarfare-Schreier.pdf

[21] STEVENS, Tim. Apocalyptic Visions: Cyber War and the Politics of Time. *Social Science Research Network* [online]. 2013, s. 28 [cit. 2015-04-25]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2256370

[22] NATO Review 2011, Nové hrozby- kybernetické dimenzie. Available from: < http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SK/index.htm>. [23 September 2014].

[23] SEKERA, Tomáš. 2008. *Kybernetické útoky: Rusko? - Gruzie a svět*. Dostupné také z: http://www.mvcr.cz/soubor/zpravodajstvi-dokumenty-prezentace-spolecnosti-logica.aspx

[24] LEWIS, J M. 2010. *Cyberwarfare and its impact on international security*. New York: United Naions Office for Disarmament Affairs, United Nations.

[25] Rosenbach M 2014*, Überwachung all over? - Von NSA zum BND und zurück, lecture notes distributed in Digitalle Schwelle at The University of Technology, Dresden on 3.7.2014.*

„Duqu“ bola zbierka počítačového malwaru, ktorá sa svojou štruktúrou a dizajnom veľmi podobala *„Stuxnetu“* a bola vytvorená na získavanie dát z organizácií spravujúcich priemyselnú infraštruktúru so zámerom spáchať v budúcnosti útok proti tretej strane. Objavený a analyzovaný bol na *„Budapest University of Technology and Economics“*. V čase, keď tam o ňom vypracovávali správu, bol s určitosťou lokalizovaný v ôsmych krajinách.[26] V roku 2012 sa stal populárnym vírus *„The Flame“*, ktorého kód je považovaný za jeden z doposiaľ najškodlivejších a najsofistikovanejších. *„The Flame“* už od roku 2010 kradol a vymazával dáta z počítačov Iránskeho ropného ministerstva, Iránskej národnej ropnej spoločnosti a ďalších organizácií sídliacich v Maďarsku, Libanone, Rakúsku, Rusku, Hong Kongu a Spojených arabských emirátoch.[27]

1.2. Čínsky cyberwarfare

1.2.1. Doktrína

„Cyberwarfare“ patrí medzi piliere čínskej bezpečnostnej stratégie už od 90. rokov dvadsiateho storočia, konkrétne od Vojny v zálive, ktorá presvedčila predstaviteľov Číny o dôležitosti a výhodách technickej a informačnej nadradenosti nad protivníkom. Na základe tejto skúsenosti začali stratégovia Čínskej ľudovej republiky takzvanú *„Revolution in Military Affairs“* tvrdiac, že v budúcnosti bude jedným z najdôležitejších pilierov vo vedení vojny odstrihnutie protivníkových informačných tokov. V neslávnom manifeste z roku 1999 nazvanom *„Unrestricted warfare“*, kolonelovia čínskej armády *„People´s Liberation Army (PLA)*“, Qiao Liang a Wang Xiangsui, hovorili o spôsobe vedenia vojny, ktorý *„prekonáva všetky hranice a limity“* a zdôraznili „*centrálnu rolu, ktorú kybernetický priestor zohráva v budúcich konfliktoch“*[28].

Mnohými spôsobmi je súčasný čínsky dôraz na *„cyberwarfare“* len rozšírením myšlienok tradičných čínskych stratégov, a to konkrétne Sun Tzu a jeho *“overcoming the superior*

[26] BENCSÁTH, Boldizsár, Gábor PÉK, Levente BUTTYÁN a Márk FÉLEGYHÁZI. 2011. *Duqu: A Stuxnet-like malware found in the wild* [online]. Budapest [cit. 2015-05-06]. Dostupné z: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. Technical Report. Budapest University of Technology and Economics.

[27] Cyber-crime, securities markets and systemic risk 2013, Joint Staff Working Paper of the IOSCO Research Department and Worlds Federation of exchanges. Alailable from: <http://www.csrc.gov.cn/pub/csrc_en/affairs/AffairsIOSCO/201307/W020130719521960468495.pdf>. [20 August 2014]

[28] MAZANEC, Brian M. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

with the inferior" a Mao C´tungovho konceptu *„People's War"*[29]. Je tiež úzko spojený s hlavnými záujmami Číny, a teda prežitím režimu, dominanciou v regióne Ázie a Pacifiku, rastúcim vplyvom na globálnej úrovni či predchádzaním nezávislosti Tajvanu a zabránením vojenskej účasti Spojených štátov v tomto konflikte[30].

Čínska doktrína *„cyberwarfare"* bola navrhnutá tak, aby obsahovala prvky americkej doktríny *„cyberwarfare"* premiešané s čínskymi kultúrnymi prvkami, ako je napríklad dávanie prednosti útoku na slabú stránku nepriateľa pred útokom na silnú stránku alebo zlatý štandard bojovania *„People´s War"*[31].

Publikácie o *„information warfare"* PLA z roku 1996 zmieňujú jeho použitie na zastrašovacie účely. V roku 2007, vrchný generál Li Deyi, miestopredseda *„Department of Warfare Theory and Strategic Research, PLA Academy of Military Science"*, vyhlásil, že informačné zastrašovanie: *„je za účelom dosiahnutia národných strategických cieľov novým módom strategického myslenia a spolu s jadrových zastrašovaním novou dôležitosťou zastrašovacou silou".*[32]

Práve takéto agresívne vyjadrovanie čínskych autorov a aktivita tímov *„Advanced Persistant Threat (APT)"*, o ktorej budem písať v nasledujúcej kapitole, je západnými analytikmi najčastejšie používaná pri snahe charakterizovať hrozby čínskeho *„cyberwarfare"*.[33]

1.2.2. Čínske kybernetické kapacity

Hlavným aktérom Číny v oblasti *„cyberwarfare"* je armáda. PLA disponuje kapacitami *„information warfare"*, ktoré sú špeciálne sústredené na *„cyberwarfare"*, a podľa doktríny

[29] People´s war je politicko-vojenská stratégia vyvinutá Mao C´tungom spočívajúca v podpore populácie a zatiahnutí nepriateľa do vnútrozemia, kde ho obyvatelia zničia prostredníctvom mobilného a gerilového warfare

[30] PERRY, William G. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *The Center for Security Policy* [online]. (28) [cit. 2015-05-05]. Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2007-10-China%20Paper%20Final%20Draft%20%282%29.pdf

[31] MAZANEC, Brian M. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

[32] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[33] Ibid

môžu byť použité aj v čase mieru.[34] Tiež vlastní vyvinutú organizačnú štruktúru pre kybernetické operácie, hlavne v rámci „*Third"* a „*Fourth Departments PLA General Staff"*. *„Third Department"* je čínskym ekvivalentom americkej Národnej bezpečnostnej agentúry (NSA) majúcim zodpovednosť za signálne spravodajstvo a obranu sietí. Predpokladá sa, že *„Third Department"* prevádzkuje taktiež tímy APT. *„Fourth Department"* je predovšetkým zodpovedné za *„electronic warfare"*, no jeho kybernetická misia nie je stále úplne jasná.[35]

Väčšina z operácií PLA sú *„Computer - Network Exploitation"* operácie realizované za účelom získavania spravodajského materiálu. Mnohí analytici sa však obávajú, že tieto už majú iba krôčik ku „*Computer - Network Attack"* operáciám, generujúc nejasnosť medzi získavaním spravodajského materiálu a útočnými operáciami. Napríklad čínske testovanie zariadení kritickej infraštruktúry ako je elektráreň v Spojených štátoch je tak agresívne, že sa táto možnosť nedá opomenúť.[36]

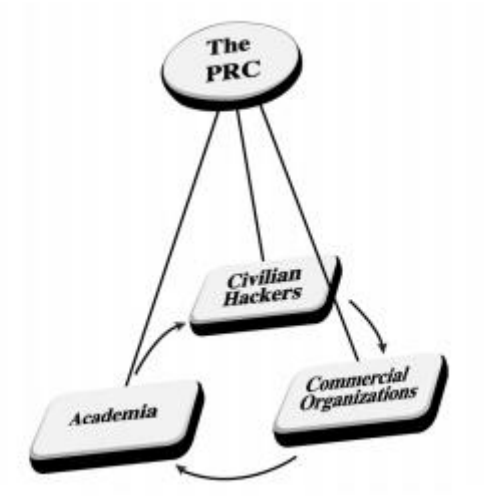
PLA tiež vyvinula nový prístup s názvom *„Integrated Network Electronic Warfare",* v rámci ktorého sú skombinované nástroje počítačových sietí a *„electronic warfare"*, a sú použité proti informačným systémom protivníka.[37]

Čo sa týka ľudského kapitálu, v súlade s Maovou doktrínou *„People's War"* zdôrazňujúcou masovú mobilizáciu občanov do vojny, sa kybernetická stratégia Čínskej ľudovej republiky opiera o prijímanie zručných operátorov informačných sietí do armády a armádnych rezerv. Verbuje pracovníkov IT, akademikov a svoje jednotky buduje aj v súkromných telekomunikačných a IT spoločnostiach. Napríklad, medzi rokmi 2003 a 2006 boli v miestnych firmách *„Guangzhou Military Region"* zriadené štyri *„Militia Information Technology battalions"* využívajúce ich personál, finančné zdroje aj vybavenie. Dôležitú úlohu v rámci čínskeho *„cyberwarfare"* zohrávajú aj hackeri, ktorí spolupracujú s armádou, aj keď ešte nie je úplne dokázané, do akej veľkej miery.[38] Čínska vláda však toto popiera

[34] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss
[35] LINDSAY, Jon R. 2014. On Cybersecurity The Impact of China on Cybersecurity. *Internal Security* [online]. (3) [cit. 2015-05-05]. Dostupné z: http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00189#.VUjmLvntmko
[36] Ibid
[37] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf
[38] Ibid

a opakovane vyhlasuje, že je striktne proti, a že zakazuje všetky ilegálne aktivity vykonávané hackermi, a že všetci, ktoré takéto aktivity páchajú, majú za ne prevziať zodpovednosť definovanú Trestným zákonom Čínskej ľudovej republiky.[39]

Obr. 1: *Aktéri „cyberwarfare" v Číne*[40]



Obrázok č. 1 znázorňuje prepojenie medzi civilnými hackermi, akadémiou a obchodnými spoločnosťami v Číne.

Od začiatku 21. storočia čínska vláda intenzívne investuje do výskumu a rozvoja a vytvára integrovaný systém spolupráce medzi obrannou, priemyslom, univerzitami a výskumnými inštitútmi. Čínska obranná politika kladie dôraz na koordinovaný vývoj hospodárstva a národnej obrany a snaží sa z národnej obrany urobiť organickú časť jej sociálneho a hospodárskeho vývoja.[41] Za účelom podpory hospodárskeho rozvoja sa uchyľuje tiež

[39] SWAINE, Michael D. 2013. Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://carnegieendowment.org/files/CLM42MS.pdf
[40] CHOI, SeulAh a Gon NAMKUNG. *State-led Back-scratching Alliance: The Chinese Government as the Umbrella* [obrázok]. In: State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era [online]. CHOI, SeulAh a Gon NAMKUNG, 2013, [vid. 2015-05-10]. č.2. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf, prevzaté
[41] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

k priemyselnej špionáži. CNE sú tým pádom využívané s dvojakým účelom - podporiť PLA a súčasne aj čínsku ekonomiku.[42]

Z predchádzajúceho textu je možné usúdiť, že ani jedna z definícií *„cyberwarfare"* nie je pre Čínu úplne platná. V Číne sa zvláštne mieša a splýva vojenský a súkromný sektor, *„cyberwarfare"* a ekonomická špionáž. Rozlíšiť medzi čínskou kybernetickou hrozbou vojenského a ekonomického charakteru je preto niekedy veľmi ťažké.

1.2.3. Porovnanie čínskych investícií do cyberwarfare s okolitými krajinami

V porovnaní s inými krajinami Čína značne investuje do *„cyberwarfare"*[43]. Nasledujúca tabuľka znázorňuje kapacity *„cyberwarfare"*, akými disponujú Čína a jej susediace štáty.

Tabuľka č. 1: *Zhrnutie národných „cyberwarfare" kapacít* [44]

	Čína	***India***	***Irán***	***Severná Kórea***	***Pakistan***	***Rusko***
Oficiálna doktrína „cyberwarfare"	**x**	**x**			**P**	**x**
Tréning „cyberwarfare"	**x**	**x**	**x**		**x**	
Cvičenia a simulácie „cyberwarfare"	**x**	**x**				
Spolupráca s IT priemyslom a technickými univerzitami	**x**	**x**	**x**		**x**	**x**
IT road map	**P**	**x**				
Jenotky „cyberwarfare"	**x**	**x**		**x**		
Záznamy o hackovaní iných štátov	**x**					**x**

P – pravdepodobne

X – áno

[42] Ibid

[43] MAZANEC, Brian M. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

[44] MAZANEC, Brian M. *Summary of nation – state cyberwarfare capabilities* [tabuľka]. In: *THE ART OF (CYBER) WAR* [online]. MAZANEC, Brian M, 2009, [vid. 2015-05-10]. č.2. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf, prevzaté dáta a upravené

Ako je možné vidieť z tabuľky, Čína disponuje oficiálnou doktrínou „cyberwarfare“, prevádzkuje tréningy a simulácie „cyberwarfare“, spolupracuje v tejto oblasti s IT priemyslom a univerzitami, pravdepodobne disponuje IT mapou ciest, jednotkami „cyberwarfare“ a sú k dispozícii záznamy jej útokov na iné štáty. Z okolitých krajín sa s ňou môže porovnávať iba India, no neexistujú záznamy o tom, že by India hackovala iné krajiny.

2. Čína ako kybernetická hrozba pre bezpečnosť USA

2.1. USA a Čína a ich vzťah v kontexte veľmocenského súperenia: história a súčasnosť

2.1.1. USA

Nie je možné pochybovať o významnej pozícii Spojených štátov amerických v súčasnom medzinárodnom systéme. Ich postavenie je formované niekoľkými základnými prvkami. Jedným z nich je pozícia, ktorú získali na základe porážky Sovietskeho zväzu v studenej, a teda poslednej hegemonickej vojne. Ďalším je ich ekonomická sila a vojenská nadradenosť. Spojené štáty dosahujú najvyšší hrubý domáci produkt na svete, sú vlastníkom svetových komunikačných sietí a databánk, je tam sústredených najviac vedecko - technických inovácií, univerzít a výskumných stredísk a prevádzajú rozsiahly vojenský výskum. USA tiež disponujú najväčšími ozbrojenými silami (do kapacity i do mobilnosti) na svete, na ktoré vydávajú až štyri percentá HDP. Sú takisto jedinou krajinou udržiavajúcou svoju celosvetovú sieť vojenských základní[45] a majú vedúce postavenie na pôde mnohých vyjednávacích fór[46]. Ďalšou z charakteristík formujúcich medzinárodné postavenie USA je export ich národných ideálov v snahe urobiť zo sveta *„lepšie a bezpečnejšie miesto“*[47], inak nazývaný aj transformačným aspektom americkej zahraničnej politiky po roku 1945 a založený na viere, že práve USA sú *„posledným strážcom medzinárodného poriadku“*.[48] S týmto je tiež spojený prvok exceptionalizmu v zahraničnej politike USA, v rámci ktorého USA samé seba vnímajú ako jedinečné. Exceptionalizmus je možné rozdeliť na tri druhy. Prvým je exemptionalistický, v rámci ktorého sa USA snažia oslobodiť sa od požiadaviek medzinárodných zmlúv a noriem, na ktorých sa predtým podieľali. Druhým je exceptionalizmus dvojitých štandardov, podľa ktorého dbajú viac na to, či sa nepriateľ správa v súlade s medzinárodnými normami, než na to, či sa podľa nich chovajú oni či ich spojenci. Tretím druhom je privilegovaný exceptionalizmus, podľa ktorého je domáca legislatíva

[45] KREJČÍ, Oscar. 2009. *Zahraniční politika USA*. Praha: Professional Publishing. ISBN 978-80-7431-003-4.
[46] FOOT, Rosemary a Andrew WALTER. 2011. *China, the United States, and global order*. 1. Cambridge: Cambridge University Press. ISBN 9780521725194.
[47] Ibid
[48] Ibid

Spojených štátov vnímaná ako legitímnejšia než tá, čo bola prejednávaná na globálnej úrovni.[49]

Donedávna bolo možné hľadieť na USA ako na jedinú svetovú mocnosť. To však viac nie je pravda. Globalizácia transformujúca svet z unipolárneho na multipolárny a dlhodobé angažovanie USA v Iraku a Afganistane, ktoré majú spojitosť s problémami s výškou rozpočtového deficitu USA, a kríza amerického modelu tržnej ekonomiky nastolili otázku týkajúcu sa udržateľnosti vedúcej pozície USA vo svete. Niektoré prieskumy napríklad ukazujú, že zahraničný verejný imidž USA od roku 2002 poklesol, a to najmä vďaka odmietavému prístupu ku krajinám a záležitostiam, ktoré nesúvisia so svetovou vojnou proti terorizmu.[50] Naopak je možné pozorovať nezanedbateľný nárast iných krajín, ako napríklad Čína, India, Brazília či Rusko a ich vzrastajúcu asertivitu v zahraničnej politike.[51]

2.1.2. Čína

V Čínskej ľudovej republike žije pätina celkovej svetovej populácie a má najväčší trh na svete. S výnimkou Južnej Ázie sú všetky hlavné medzinárodné regióny veľkosťou populácie menšie ako Čína.[52] Okrem svojej veľkosti je Čína významná aj svojou ekonomickou silou. Zatiaľ, čo v USA bojovali s krachujúcimi bankami, prehlbujúcim sa deficitom federálneho rozpočtu či platobnou neschopnosťou miest a štátov, čínska ekonomika vykazovala nárast tempom až okolo 9 až 10 percent. V roku 2011 sa stala druhou najväčšou ekonomikou sveta tým, že jej objem predstihol objem japonskej ekonomiky a je očakávané, že v priebehu jedného desaťročia sa stane väčšou než ekonomika USA.[53] Svojím ekonomickým rastom je s ňou z krajín BRICu porovnateľná iba India.[54] Ekonomický rast ide ruka v ruke s modernizáciou Čínskej oslobodeneckej armády, do ktorej v posledných rokoch

[49] FOOT, Rosemary a Andrew WALTER. 2011. *China, the United States, and global order*. 1. Cambridge: Cambridge University Press. ISBN 9780521725194.

[50] LUM, Thomas, Christopher M. BLANCHARD, Nicolas COOK a Kerry DUMBAUGH. 2010. *China in the 21st Century : China and the U.S. : Comparing Global Influence* [online]. [cit. 2015-05-05]. ISBN 9781616689841. Dostupné z: http://site.ebrary.com/lib/natl/reader.action?docID=10674905

[51] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[52] WOMACK, Brantly. 2010. *China among unequals: asymmetric foreign relationships in Asia*. 1. Singapore: World Scientific. ISBN 978-9814295277.

[53] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[54] KWANG, Ho Chun a . 201n. l. *BRICs Superpower Challenge : Foreign and Security Policy Analysis* [online]. Ashgate Publishing Ltd [cit. 2015-05-05]. ISBN 9781409468707. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

Čína vkladá desať percent zo svojho rozpočtu.[55] Čo sa týka zahraničnej politiky, je možné zhodnotiť, že za poslednú jeden a pol dekádu *„soft power"* Číny na medzinárodnej úrovni značne vzrástla a Čína sa z demoralizovanej, izolovanej a ochudobnenej krajiny stala sebavedomou, asertívnou a prosperujúcou obchodnou mocnosťou.[56] Zaslúžil sa o to hlavne fakt, že od polovice deväťdesiatych rokov dvadsiateho storočia sa Čínska ľudová republika snaží o adoptovanie stále viac aktívneho a pragmatického diplomatického prístupu ku svetu zdôrazňujúceho hlavne ekonomické záujmy. Propagujúc obchod, investície, diplomatické výmeny, turizmus[57] a zahraničnú pomoc, získava nové odbytištia pre svoje produkty, prístup k nerastným surovinám a medzinárodné uznanie.[58] Z pohľadu medzinárodnej bezpečnosti je možné povedať, že čínska zahraničná politika sa predovšetkým riadi tradičnou teóriou rovnováhy síl, ktorej prioritou je udržanie teritoriálnej integrity a suverenity v multipolárnom svete[59]. Tiež sa dá zhodnotiť, že Čína kopíruje stratégiu a taktiku USA v tom, že sa snaží chrániť územia, ktoré sa nachádzajú pod jej vplyvom a či už politicky, kultúrne alebo ekonomicky vplývať na oblasti, o ktoré má záujem.[60] Nárast čínskeho vplyvu môžeme pozorovať hlavne v strednej Ázii, o ktorú sa zaujíma predovšetkým z geopolitických dôvodov. Zasadzuje sa o koniec rozširovania amerických vojsk v oblasti z dôvodu strachu z možného obkľúčenia Číny. Zvyšovanie vplyvu v strednej Ázii môžeme vidieť na príklade rozsiahlych investícií do ropného, uránového a plynového priemyslu Turkmenistanu a Kazachstanu.[61] Pozorovatelia z mnohých kruhov veria, že v budúcnosti by Čínska ľudová republika mohla nahradiť Spojené štáty ako svetovú veľmoc, presne tak, ako kedysi USA

[55] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[56] KWANG, Ho Chun a . 201n. l. *BRICs Superpower Challenge : Foreign and Security Policy Analysis* [online]. Ashgate Publishing Ltd [cit. 2015-05-05]. ISBN 9781409468707. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

[57] KWANG, Ho Chun a . 201n. l. *BRICs Superpower Challenge : Foreign and Security Policy Analysis* [online]. Ashgate Publishing Ltd [cit. 2015-05-05]. ISBN 9781409468707. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

[58] LUM, Thomas, Christopher M. BLANCHARD, Nicolas COOK a Kerry DUMBAUGH. 2010. *China in the 21st Century : China and the U.S. : Comparing Global Influence* [online]. [cit. 2015-05-05]. ISBN 9781616689841. Dostupné z: http://site.ebrary.com/lib/natl/reader.action?docID=10674905

[59] KWANG, Ho Chun a . 201n. l. *BRICs Superpower Challenge : Foreign and Security Policy Analysis* [online]. Ashgate Publishing Ltd [cit. 2015-05-05]. ISBN 9781409468707. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

[60] ŠTEFANCOVÁ, Vladimíra a René PAWERA. 2013. ČÍNA A SÚČASNÝ MANAŽMENT MEDZINÁRODNEJ BEZPEČNOSTI. *Academia.edu* [online]. [cit. 2015-05-05]. Dostupné z: http://www.academia.edu/6616164/%C4%8C%C3%8DNA_A_S%C3%9A%C4%8CASN%C3%9D_MANA%C5%BDMENT_MEDZIN%C3%81RODNEJ_BEZPE%C4%8CNOSTI

[61] Ibid

nahradili Anglicko. Tieto predpoklady vychádzajú z konzervatívnych, nacionalistických, liberalistických, internacionalistických i izolacionistických kruhov.[62]

2.1.3. Vzťah USA a Číny

Od vzniku Čínskej ľudovej republiky v roku 1949 sa jej vzťah so Spojenými štátmi americkými asi najvýstižnejšie dá nazvať premenlivým.

Po skončení druhej svetovej vojny Spojené štáty odmietali uznať existenciu komunistickej Čínskej ľudovej republiky. Čína sa stala predmetom politiky *„containmentu"*[63] a po väčšinu rannej fázy studenej vojny bola považovaná za hrozbu pre americkú bezpečnosť a nekomunistickú spoločnosť.[64] Ako oficiálny zástupca Číny bol považovaný Tajvan, a to aj napriek tomu, že jeho vláda bola Washingtonom opakovane označená za skorumpovanú a diktátorskú. V Číne boli USA v tomto období považované za nepriateľa čínskej revolúcie[65].

Od polovice 60. rokov sa začal meniť spôsob, akým Spojené štáty vnímali Čínu. Vláda USA o Čínskej ľudovej republike prestala hovoriť ako o komunistickej a nový čínsky premiér bolo videný ako modernizátor a ten, ktorý chce Čínu urobiť *„americkejšou"*,[66] hoci stále bola komunistickým režimom a jej ekonomické a vojenské kapacity sa nezmenili.[67]

V 70. a 80. rokoch Washington obnovil diplomatické vzťahy s Čínskou ľudovou republikou a boli zintenzívnené politické, obchodné a kultúrne výmeny.[68] Diplomatické styky medzi týmito dvomi krajinami boli nadviazané konkrétne na prelome rokov 1978 – 1979, a to v kontexte americko – sovietskeho súperenia.[69]

Po politickej búrke na Tiananmenskom námestí a zmenách v Sovietskom bloku v roku 1989 Deng Xiaoping presadzoval opatrný a nekonfrontačný prístup k USA známy ako *„taoguangyanghu"* alebo snaha neupozorniť na seba prameniaci z vedomia, že medzinárodný

[62] LUM, Thomas, Christopher M. BLANCHARD, Nicolas COOK a Kerry DUMBAUGH. 2010. *China in the 21st Century : China and the U.S. : Comparing Global Influence* [online]. [cit. 2015-05-05]. ISBN 9781616689841. Dostupné z: http://site.ebrary.com/lib/natl/reader.action?docID=10674905

[63] Vojenská stratégie, ktorej cieľom je zastavenie expanzie nepriateľa

[64] TURNER, Oliver. 2014. *American images of China: identity, power, policy*. 1. London: Routledge. ISBN 9780415659550.

[65] Ibid

[66] Ibid

[67] Ibid

[68] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[69] Ibid

status Číny je omnoho nižší než ten USA. Túto myšlienku po Deng Xiaopingovi nasledovali ešte dvaja jeho nástupcovia: Jiang Zemin a Hu Jintao.[70]

Na Jiangovom summite vo Washingtone v roku 1997 sa Čína pokúsila s USA nadviazať *„konštruktívne strategické partnerstvo“* podobné tým, aké mala aj s inými štátmi. Toto partnerstvo nabralo realistickejší ráz s nárastom vzájomných nezhôd v rokoch 1999 a 2001, kedy sa tieto štáty pokúšali postaviť svoj vzťah na konštruktívnom a úprimnom dialógu. Po teroristických útokoch z roku 2001 v rámci spoločného postoja k boju proti terorizmu Čína povolila zriadenie kancelárie právneho ataše FBI v Pekingu a uvalila vážnejšie obmedzenia na prevoz komponent zbraní hromadného ničenia, snažiac sa, aby jej záujmy čo najviac korešpondovali so záujmami Spojených štátov [71].

Za vlády Georga W. Busha bol založený *„Strategický ekonomický dialóg“* a *„Senior Dialóg“* za účelom prejednávania hospodárskych a strategických záležitostí stredného významu pre vzájomný vzťah týchto dvoch štátov, a tiež svetový a regionálny poriadok.[72] Centrálnou požiadavkou na udržanie tejto spolupráce bolo pre USA to, že Čína musí jednať ako zodpovedný aktér.[73]

V roku 2007, na začiatku svojho prvého prezidentského obdobia, Barack Obama vyhlásil, že Čínu nepovažuje za priateľa ani nepriateľa Spojených štátov, ale za ich súpera. Toto vnímanie sa neskôr začalo postupne meniť. Počas svojej prvej prezidentskej návštevy Číny zdôraznil, že uprednostňuje spoluprácu s Čínou pred konfrontáciou. Predtým spolupracoval s prezidentom Hu Jintaom na vytvorení *„US – China Strategic and Economic Dialogue“*.[74] Je možné zhrnúť, že za prvého Obamovho prezidentského obdobia bola Čína vnímaná ako *„rastúca“* a *„nezápadná“* a vzťah Číny a USA bol založený na pozitívnom jednaní a vzájomnej závislosti.[75]

Na začiatku druhého prezidentského obdobia Baracka Obamu bola Čína označená za krajinu, ktorá nedodržiava pravidlá a bola kritizovaná za nedodržiavanie autorských práv,

[70] LIEBERTHAL, Kenneth Lieberthal a Wang JISI. THE JOHN L. THORNTON CHINA CENTER AT BROOKINGS. *Addressing U.S.-China Strategic Distrust* [online]. 2012 [cit. 2014-05-18]. Dostupné z: http://www.brookings.edu/~/media/research/files/papers/2012/3/30%20us%20china%20lieberthal/0330_china_lieberthal.pdf

[71] FOOT, Rosemary a Andrew WALTER. 2011. *China, the United States, and global order*. 1. Cambridge: Cambridge University Press. ISBN 9780521725194.

[72] Ibid

[73] Ibid

[74] TURNER, Oliver. 2014. *American images of China: identity, power, policy*. 1. London: Routledge. ISBN 9780415659550.

[75] Ibid

praktizovanie *„cyberwarfare“* pomocou hackerských útokov na počítačové systémy Spojených štátov či manipuláciu meny. Táto kritika bola prezentovaná predovšetkým Mittom Romneym.[76]

Čo sa týka obchodu, Čína je druhým najväčším obchodným partnerom USA a tretím najväčším exportným trhom.[77] Tento vzťah stále narastá na svojom objeme, no je do veľkej miery ovplyvňovaný nerovnováhou, za ktorú je obviňovaná predovšetkým Čína. Z veľkej časti má totižto byť následkom čínskej menovej politiky, nevýhodných podmienok pre zahraničné spoločnosti, ktoré majú záujem podnikať v Číne, čínskeho podporovania štátnych podnikov, subvencií exportu, priemyselnej špionáže či nedodržiavania autorských práv.[78]

Výrazným faktorom hrajúcim v prospech Číny bola hospodárska a finančná kríza 2008 – 2009, vďaka ktorej sa USA, odkiaľ vzišla, stali závislými na kupovaní „*US Treasury debt*“ zahraničnými aktérmi, medzi ktorých patrila aj Čína.[79] Táto kríza zmenšila americkú dôveru vo vlastný hospodársky model, kým na druhú stranu sa ekonomický model Číny zdá relatívne robustný a jej vláda je schopná prijímať rozhodnutia podporujúce udržanie hospodárskeho rastu.[80]

Vo všeobecnosti je možné zhrnúť, že Čína akceptuje fakt, že Spojené štáty majú vo svete dominantnú pozíciu a verí, že tomu bude takto ešte niekoľko desaťročí. Uvedomuje si, že za USA zaostáva vo všetkých dimenziách moci. Napriek tomu sa však snaží o svoj vlastný rast, viac a viac sa integruje do svetového hospodárstva, profituje z globalizácie a zvyšuje svoje vojenské výdaje.[81]
Peking ale tiež zastáva presvedčenie, že Washington nechce, aby sa Čína stala svetovou mocnosťou a je schopný urobiť čokoľvek, aby obmedzil ekonomický rast Číny, resp. mu úplne zabránil, a tiež, aby zabránil rastu čínskej vojenskej moci. Toto presvedčenie sa zakladá na vzájomnej nedôvere medzi týmito dvomi štátmi prameniacej predovšetkým z histórie

[76] Ibid

[77] SWAINE, Michael D. a . 201n. l. *America's Challenge : Engaging a Rising China in the Twenty-First Century* [online]. Carnegie Endowment for International Peace [cit. 2015-05-05]. ISBN 9780870032585. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

[78] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[79] FOOT, Rosemary a Andrew WALTER. 2011. *China, the United States, and global order*. 1. Cambridge: Cambridge University Press. ISBN 9780521725194.

[80] Ibid

[81] Ibid

a z toho, ako sú interpretované niektoré súčasné postupy Spojených štátov v tichomorskej oblasti.[82] Washington sa evidentne skutočne snaží limitovať čínsky regionálny aj globálny vplyv, a to napríklad posilňovaním bezpečnostných vzťahov so všetkými štátmi obklopujúcimi Čínu, odmietaním predaja vojenského vybavenia Pekingu či svojím blízkym vzťahom s Tajvanom. V tomto prístupe znova vidíme politiku *„containmentu"* podobnú tej za studenej vojny.[83] Čo sa týka Číny, USA jedná v súlade so svojimi záujmami, ktorými sú, ako vyhlásila Hillary Clinton, udržať vedúce postavenie Spojených štátov vo svete, zaistiť vlastné záujmy a šírenie hodnôt USA v regióne.[84]

2.2. Čína ako kybernetická hrozba pre bezpečnosť USA

V posledných rokoch sa kybernetická bezpečnosť stala vo vzájomnom vzťahu Spojených štátov amerických a Číny veľmi dôležitou a bežnou témou. Spojené štáty si uvedomujú závislosť svojej armády, infraštruktúry a hospodárstva na informačných technológiách a aj ich ľahkú zraniteľnosť, a preto sa obávajú čínskych pokrokových kapacít v kybernetickom priestore. Čínu považujú za jednu z vedúcich svetových kybernetických mocností, ktorá intenzívne pracuje na vývoji kapacít schopných poraziť alebo zastrašovať USA v a pomocou kybernetického priestoru.[85]

Čína si je svojich schopností vedomá. Napriek tomu však svoje kybernetické aktivity zvykne popierať a Čínske ministerstvo zahraničných vecí a Ministerstvo obrany trvajú na tom, že Čína sama je najväčšou obeťou kybernetických útokov. Množstvo štatistík útokov na svoje informačné systémy prezentuje predovšetkým čínska armáda, pravdepodobne v snahe vyvrátiť podozrenia, že práve ona stojí za mnohými kybernetickými útokmi na iné entity.[86]

---

[82] FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

[83] TURNER, Oliver. 2014. *American images of China: identity, power, policy*. 1. London: Routledge. ISBN 9780415659550.

[84] Ibid

[85] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[86] SWAINE, Michael D. a . 201n. l. *America's Challenge : Engaging a Rising China in the Twenty-First Century* [online]. Carnegie Endowment for International Peace [cit. 2015-05-05]. ISBN 9780870032585. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

Vláda Spojených štátov tvrdí, že čínske útoky na citlivé informácie o národnej bezpečnosti a na súkromné ekonomické dáta sú na vzostupe. Čína bola za poslednú jeden a pol dekádu obvinená z veľkého množstva kybernetických útokov v podobe špionáže, krádeží dát či odmietnutia služieb. Domnieva sa tiež, že Čína svoje kapacity v kybernetickom priestore nevyužíva len na hromadenie dát za ekonomickými účelmi, no tiež na vojenské účely a ovplyvňovanie výsledkov konvenčných ozbrojených konfliktov.[87] Veľmi veľa nekalých kybernetických aktivít je vykonávaných tiež z USA. Ministerstvo obrany USA aj Čínska ľudová armáda hľadia na kybernetický priestor ako na novú bojovú doménu a jeden na druhého sa pozerajú s nedôverou.[88]

Tézou nasledujúcej časti práce je to, že Čína svojím svojim správaním v kybernetickom priestore ohrozuje Spojené štáty dvomi základnými spôsobmi. Prvým z nich je to, že svojou kybernetickou ekonomickou špionážou systematicky rozkladá konkurencieschopnosť firiem USA a iných západných krajín. Druhý spôsob je schopnosť Číny na nízke náklady paralyzovať vojenské vedenie a kontrolu a kritickú infraštruktúru Spojených štátov[89].

Ako už bolo naznačené v predchádzajúcej kapitole, čínsku ekonomickú a vojenskú hrozbu pre USA je zložité od seba úplne oddeliť. Čínska kybernetická hrozba je výsledkom spolupráce verejného a súkromného sektoru; spolupráce vlády, armády, súkromných firiem, univerzít a hackerov. Čínska obranná politika sa snaží o koordinovaný vývoj hospodárstva a národnej obrany.[90] Kybernetické útoky sú teda využívané s cieľom podporiť armádu a súčasne tiež čínsku ekonomiku.[91] Väčšina čínskej ekonomickej špionáže je namierená na americké komerčné ciele, ktoré majú nejakú spojitosť s vojenskou technológiou. Napríklad, v roku 2011 bola napadnutá bezpečnostná spoločnosť *„RSA Security“* a ukradnuté technológie boli využité na preniknutie do vojensko-priemyselných cieľov. Krátko potom boli napadnuté siete *„Lockheed Martin“*[92], ktorý využíval bezpečnostné tokeny RSA. [93]

[87] MAZANEC, Brian M. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

[88] *China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops held at the University of California, San Diego*. 2012. Dostupné také z: http://igcc.ucsd.edu/assets/001/503541.pdf

[89] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[90] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[91] Ibid

[92] Výrobca rakiet a lietadiel

2.2.1. Hrozba ekonomického charakteru

V súčasnosti sa zdá, že Spojené štáty považujú za urgentnejšiu čínsku ekonomickú než vojenskú kybernetickú hrozbu. Nové spravodajské odhady tvrdia, že USA sú cieľom masívnej udržiavanej kybernetickej špionážnej kampane ohrozujúcej konkurencieschopnosť krajiny.[94] Za posledných päť rokov sa obeťou hackerov stali rozličné sektory ekonomiky: energetický, finančný, informačných technológií, automobilový, vesmírny. Tiež noviny ako *„The New York Times", „The Wall Street Journal"* a *„The Washington Post"* veria, že Číňania útočia na ich siete.[95] Podľa „*REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION"* z roku 2014 sú ročné náklady spôsobené kybernetickým zločinom v USA vyhodnotené na 24 až 120 biliónov dolárov, čo znamená 0,2 až 0,8 percent HDP, čo vyúsťuje do straty približne 200, 000 pracovných miest ročne.[96]

Má sa za to, že prevažná časť kybernetickej špionáže z Číny je realizovaná *„People´s Liberation Army"*, ktorá má prevádzkovať takzvanú Unit 61398, nazývanú aj tím APT1[97].

APT

Od roku 2005 *„Mandiant"*[98] zaznamenáva výrazné zmeny týkajúce sa oblasti kybernetických bezpečnostných incidentov. Výnimočne schopným tímom útočníkov, ktoré sú zrejme dobre financované, sa úspešne darí napádať vládne organizácie, organizácie vykonávajúcu činnosť spojenú s obranou štátu, výskumné, výrobné a právnické firmy či neziskové organizácie. *„Mandiant"* tieto tímy nazval APT (*„Advanced Persistent Threat").* Podľa *„Mandiantu"* APT nie sú len obyčajnými hackermi. Sú to profesionáli so skutočne vysokou mierou úspešnosti, ktorí dokážu prekonať mnoho bezpečnostných opatrení. Okrem kradnutia dát je

[93] NAKASHIMA, Ellen. 2013. US Target of Massive Cyber- Espionage Campaign. *Washington Post* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://www.ctcitraining.org/docs/US_Target_of_Massive_Cyber_Espionage_Campaign.pdf

[94] NAKASHIMA, Ellen. 2013. US Target of Massive Cyber- Espionage Campaign. *Washington Post* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://www.ctcitraining.org/docs/US_Target_of_Massive_Cyber_Espionage_Campaign.pdf

[95] Ibid

[96] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[97] MANDIANT. *APT1 Exposing One of China's Cyber Espionage Units*. 2013. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[98] spoločnosť zaoberajúca sa informačnou bezpečnosťou. Správy Mandiantu boli podporované US Department of Homeland Security, ktoré im poskytlo internetové adresy hackerských skupín v Číne.

cieľom týchto tímov vytvoriť cestu, ktorou sa do napadnutých systémov dokážu znovu vrátiť, ukradnúť dodatočné dáta a ostať pre obeť neidentifikovateľní. Základné atribúty týchto útokov naznačujú, že sú sponzorované štátom[99].

V správe z roku 2010 *„Mandiant"* zhodnotil, že čínska vláda je schopná autorizovať tieto aktivity, no nedá sa zistiť, do akej miery je v útokoch zaangažovaná. Každopádne, v každom prípade, ktorý *„Mandiant"* skúmal, bolo možné určiť nejakú spojitosť medzi prevedeným útokom a súčasným dianím v Číne[100]. V správe z roku 2013 už *„Mandiant"* uvádza, že APT tímy sa nachádzajú hlavne v Číne, a že čínska vláda je s nimi oboznámená. Priamo z Číny pochádza viac než dvadsať APT tímov [101].

APT 1

APT 1 je údajne podporovaný čínskou vládou a venuje sa kybernetickej špionáži. Patrí medzi najväčšie hrozby pre kybernetickú bezpečnosť pochádzajúce z Číny, a tiež medzi skupiny, ktorým sa podarilo ukradnúť najväčšie množstvo dát.[102]

Správa *„Mandiantu"* z roku 2013[103] poskytuje o APT 1 nasledujúce závery:

- *„Mandiat"* verí, že tento tím je súčasťou Ľudovej oslobodeneckej armády a je známy ako Unit 61398.
- APT 1 mal systematicky ukradnúť stovky terabajtov dát z najmenej 141 organizácií a preukázal svoju schopnosť a záujem kradnúť z tuctov organizácií súčasne.
- APT 1 sa sústreďuje na široké spektrum organizácií v anglicky hovoriacom svete.
- APT 1 udržiava rozsiahlu infraštruktúru počítačových systémov po celom svete.
- Vo viac než 97 percent z 1905 krát, čo *„Mandiant"* pozoroval APT 1 útoky s cieľom skúmať infraštruktúru útoku, APT 1 použilo IP adresy registrované v Šanghaji a systémy nastavené na používanie zjednodušenej formy čínskeho jazyka.
- Veľkosť APT 1 naznačuje, že sa jedná o veľkú organizáciu prinajmenšom s tuctami, ale potenciálne so stovkami ľudských operátorov.

[99] MANDIANT. 2010. *The Advanced Persistent Threat*. Dostupné také z: https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf

[100] Ibid

[101] MANDIANT. *APT1 Exposing One of China's Cyber Espionage Units*. 2013. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[102] Ibid

[103] MANDIANT. *APT1 Exposing One of China's Cyber Espionage Units*. 2013. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

- Za účelom zdôrazniť, že útočníkmi sú skutočné osoby, *„Mandiant“* odhalil tri postavy spojené s aktivitou APT 1: *„UglyGorilla“, „DOTA“* a *„SuperHard“*.
- Mandiant uvoľnil viac než 3000 indikátorov na podporu obrany proti APT 1 operáciám.[104]

Okrem ekonomickej špionáže, ktorou sa v tejto práci hlavne zaoberám, je ekonomickou hrozbou pre USA tiež čínska internetová a mediálna kontrola a jej negatívny vplyv na spoločnosti Spojených štátov.

Podľa *„REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*“ sú americké spoločnosti stále viac a viac ovplyvňované čínskou reštriktívnou kontrolórskou politikou. Facebook, Twitter a YouTube sú v Číne zablokované, predovšetkým kvôli ich neochote cenzurovať obsah. Ako následok tieto americké spoločnosti strácajú obrovské podnikateľské príležitosti a sú nahradzované čínskymi firmami ako Weibo, RenRen, a Youku.[105]

Čínska vláda už dlho udržuje silnú kontrolu nad tradičnými aj novými médiami s cieľom vyhnúť sa snahám o podkopanie jej autority[106] a zabrániť šíreniu nepravých politických zvestí.[107] Medzi ich taktiky patrí napríklad prísna kontrola médií za pomoci monitorovacích systémov a firewallov, vymazávanie publikácií a webových stránok a zatýkanie disidentných novinárov, blogerov a aktivistov[108]. Podľa čínskych používateľov internetu cenzori okrem odkazov s politicky zameranou tematikou cenzurujú aj pojmy ako sloboda, tvorba, mier, hypermarket, tibetttalk či Hlas Ameriky.[109] V roku 2013 sa Čína v rebríčku Reportérov bez hraníc skúmajúcom indexy slobody tlače zaradila až na 173. zo 179. miest[110]. Uväznený

[104] MANDIANT. *APT1 Exposing One of China's Cyber Espionage Units*. 2013. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[105] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[106] BEINA, Xu. 2014. Media Censorship in China. *Council on Foreign Relations* [online]. [cit. 2015-05-11]. Dostupné z: http://www.cfr.org/china/media-censorship-china/p11515

[107] FISHMAN, Ted. 2006. *China, Inc.: jak Čína drtí Ameriku a svět*. 1. Praha: Alfa Publishing. ISBN 9788086851440.

[108] BEINA, Xu. 2014. Media Censorship in China. *Council on Foreign Relations* [online]. [cit. 2015-05-11]. Dostupné z: http://www.cfr.org/china/media-censorship-china/p11515

[109] FISHMAN, Ted. 2006. *China, Inc.: jak Čína drtí Ameriku a svět*. 1. Praha: Alfa Publishing. ISBN 9788086851440.

[110] BEINA, Xu. 2014. Media Censorship in China. *Council on Foreign Relations* [online]. [cit. 2015-05-11]. Dostupné z: http://www.cfr.org/china/media-censorship-china/p11515

čínsky aktivista Liu Xiaobo bol dokonca v roku 2010 odmenený Nobelovou cenou za to, že dokázal medzinárodné spoločenstvo upozorniť na problém s cenzúrou médií v krajine[111].

2.2.2. Hrozba vojenského charakteru

Ako tu už bolo spomenuté, Spojené štáty sú mocnosťou, ktorá je v oblasti konvenčnej aj jadrovej sily neporaziteľná. Ich technologická nadradenosť z nich robí ale aj krajinu, ktorá je najzraniteľnejšia kybernetickým útokom. Texty čínskych vojenských autorov o *„cyberwarfare"* aj čínske kybernetické kapacity a technologický rozvoj dávajú USA dôvod na obavy. Vzhľadom na časté agresívne konanie Číny voči USA v kybernetickom priestore, môžu byť tieto obavy opodstatnené.

Nasledujúca tabuľka obsahuje zoznam vybraných údajných kybernetických útokov Číny na USA, ktoré je možné nazvať *„cyberwarfare"*. Následne sú niektoré z nich opísané.

Tabuľka č. 2: *Prípady čínskeho „cyberwarfare" proti USA*[112]

Máj 1999	Zničenie webových stránok vlády Spojených štátov po bombardovaní čínskej ambasády v Srbsku	**Leto 2006**	Útok na počítače *„Commerce Department's Bureau of Industry and Science"*
Apríl 2001	*„The First Sino-American cyber warfare"* po havárii špionážneho lietadla USA s čínskym bojovým lietadlom	**November 2006**	Útok na počítačovú infraštruktúru *„US Naval War College"*
Máj 2002	Pamiatka *„The First Sino-American cyber warfare"*	**Zima 2006**	Útok na počítačové banky (computer banks) na *„U.S. National Defense University"* uprostred veľkej simulácie elektronickej vojny

[111] Ibid
[112] CHOI, SeulAh a Gon NAMKUNG. *The Cases of China's Cyber Warfare against the United States* [tabuľka]. In: State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era [online]. CHOI, SeulAh a Gon NAMKUNG, 2013, [vid. 2015-05-10]. č.2. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf; prevzaté dáta a upravené

November 2004	Preniknutie do mnohých odtajnených vojenských systémov USA	**Jún 2007**	Preniknutie do emailového systému *„Secretary of Defense“*
August 2005	Preniknutie do počítačových systémov Ministerstva obrany Spojených štátov nazvané *„Titánový dážď“*	**Október 2007**	Zaslanie emailov so škodlivými prílohami do *„Oak Ridge National Lab“*
Júl 2006	Preniknutie do sietí *„US Department of State“*	**November 2008**	Preniknutie do informačného systému Bieleho domu
August 2006	Penetrácia do NIPRET (Non-classified Internet Protocol Router Network)	**November 2008**	Preniknutie do najkritickejších stránok NASA vrátane Kennedyho vesmírneho centra
August 2006	Penetrácia do počítačov konzervatívnych kongresmanov kritizujúcich čínske dodržiavanie ľudských práv	**2009**	Útok na Google a 34 ďalších organizácií zahŕňajúcich aj spoločnosti spojené s administratívou Spojených štátov či dodávateľov Pentagonu.

„The First Sino-American cyber warfare“ sa odohral v apríli 2001. V tomto mesiaci sa nad Čínou zrazili americké špionážne a čínske bojové lietadlo. Američania núdzovo pristáli a Číňania sa stratili v mori. Obidve krajiny sa za spôsobenie tej havárie navzájom vinili. Technicky zruční občania Spojených štátov vyjadrovali svoj hnev nad zadržaním posádky lietadla na internete a zmazali okolo 65 čínskych webových stránok. Ako odpoveď čínski hackeri vyhlásili USA vojnu a týždeň od prvého do siedmeho mája 2001 nazvali týždňom *„Hack the USA“* a napadli vyše 1000 stránok v USA, zahŕňajúc aj stránky Bieleho domu

či *„US Air Force“*. Tieto stránky boli buď vypnuté, alebo bol ich obsah nahradený obrázkom čínskej červenej vlajky[113].

Za asi najznámejší z týchto útokov sa dá považovať *Titánový dážď*, ktorý trval od roku 2003 do roku 2005. Boli napadnuté stovky počítačov vlády Spojených štátov a počítačové siete amerických západných spojencov. Podľa médií útok pochádzal z čínskej provincie Guangdong a podľa neoficiálnych vyhlásením úradníkov Spojených štátov to mohol byť štátom sponzorovaný CNE útok so zámerom získania obrovského množstva citlivých dát.[114]

Ďalším z prípadov je útok na NIPRNET z roku 2006, kedy sa čínskej občianskej skupine podarilo preniknúť do *„Non-classified Internet Protocol Router Network* (NIPRNET)*“* a stiahnuť odtiaľ až 20 terabytov dát. NIPRENT patrí medzi hlavné logistické siete *„US Department of Defense“* podporujúcou operácie velenia a kontroly. Hoci bol tento útok realizovaný civilnými hackermi a skupinami, jeho rozsah a použité zdroje naznačujú, že bol sponzorovaný čínskou vládou. Dôvod, prečo sa domnieva, že je v tom angažovaná aj čínska vláda je tiež ten, že na to, aby bol úspešný, neboli podporní len hackeri, ale aj iné entity, ako napríklad vojenskí a strategickí plánovači, politickí experti špecializujúci sa na čínsko-americké vzťahy a podobne.[115]

Medzi najznámejšie prípady podobného charakteru určite tiež patrí ten na Google z roku 2009, pri ktorom bolo vedenie spoločnosti napadnuté spearfishingovým útokom. Po jeho vystopovaní späť na server sa podarilo zistiť, že obeťou sa nestal len Google ale prinajmenšom 34 ďalších organizácií zahŕňajúcich Adobe, Dow Chemical, Northrop-Grumman[116], spoločnosti spojené s administratívou Spojených štátov či dodávateľov Pentagonu. Útok je pripisovaný APT a spájané sú s ním aj dve vzdelávacie inštitúcie: *„Lanxiang Vocational School“* v Jinan, Shandong province a *„Jiaotong University“*

[113] CHOI, SeulAh a Gon NAMKUNG. State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era. *The Korean Journal of International Studies* [online]. 2013, č. 2 [cit. 2015-04-26]. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf
[114] MAZANEC, Brian M.. *THE ART OF (CYBER) WAR* [online]. 2009, č. 2 [cit. 2015-04-25]. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf
[115] CHOI, SeulAh a Gon NAMKUNG. State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era. *The Korean Journal of International Studies* [online]. 2013, č. 2 [cit. 2015-04-26]. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf
[116] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

v Shanghai. Hlavným cieľom tohto útoku bolo údajne získanie informácií o čínskych separatistoch.[117]

„2012 Defense Science Board report“ identifikovala tucty kritických informačných systémov kompromitovaných čínskymi aktérmi, zahŕňajúc napríklad *„the Patriot Advanced Capability-3 air defense system“, „the F–35 and the F/A–18 fighter aircraft“, „the P–8A reconnaissance aircraft“, „the Global Hawk UAV“, „the Black Hawk helicopter“, „the Aegis Ballistic Missile Defense System“* a *„the Littoral Combat Ship“*. Táto správa tiež odhalila, že čínski kybernetickí aktéri dostali informácie o rôznych technológiách Ministerstva obrany USA, ako napríklad video o systémoch drónov, satelitnej komunikácii či systémoch *„electronic warfare“*. Kradnuté nie sú len informácie o dizajne týchto zbraní, ale napríklad a j interná komunikácia vo firmách či informácie o zamestnancoch.[118]

Na základe mnohých z vyššie uvedených útokov možno usúdiť, že Čína pomocou útokov na nižšej úrovni testovala kybernetickú obranu Spojených štátov. *„2006 Report to Congress of the U.S.-China Economic and Security Review Commission“*[119] zaraďuje tieto aktivity do programu *„kybernetickej rozviedky“,* v rámci ktorého Čína testuje počítačové siete amerických vládnych agentúr a súkromných organizácií, hľadá v nich slabé miesta a snaží sa zistiť, ako myslia americkí vodcovia, objaviť vzorce v komunikácii vládnych a súkromných organizácií a dostať sa k tajným informáciám.[120]

Samozrejme, na to, aby Čína mohla podobné útoky realizovať, musí mať k dispozícii potrebné prostriedky. Podľa Pentagonu PLA disponuje jednotkami tvoriacimi počítačové vírusy, ktoré majú útočiť na počítačové systémy a siete nepriateľa a namierené sú predovšetkým na americkú armádu. Jeden z typov týchto vírusov sa nazýva Myfip, obyčajne je veľmi dobre zamaskovaný, a v prípade, že sa dostane do slabšie chránených informačných

[117] LINDSAY, Jon R. 2014. On Cybersecurity The Impact of China on Cybersecurity. *Internal Security* [online]. (3) [cit. 2015-05-05]. Dostupné z: http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00189#.VUjmLvntmko

[118] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[119] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2006. Dostupné z: http://www.uscc.gov

[120] PERRY, William G. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *The Center for Security Policy* [online]. (28) [cit. 2015-05-05]. Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2007-10-China%20Paper%20Final%20Draft%20%282%29.pdf

systémov, je v nich schopný spôsobiť obrovské škody a ukradnúť akýkoľvek z nasledujúcich formátov súborov:[121]

.pdf – Adobe Portable Document Format • .doc – Microsoft Word Document • .dwg – AutoCAD drawing • .sch – CirCAD schematic • .pcb – CirCAD circuit board layout • .dwt – AutoCAD template • .dwf – AutoCAD drawing • .max – ORCAD layout • .mdb – Microsoft database.[122]

Každá organizácia, ktorej informačný systém je infikovaný Myfipom teda prichádza o svoje organizačné dokumenty, plány, internú komunikáciu či databáze. Počas jedného z útokov sa podarilo vystopovať jeho pôvod a to do Tianjin City v Čínskej ľudovej republike[123].

Podľa správy Pentagonu *„2006 Report on the Military Power of the People's Republic of China"* Čína pracuje na zaistení toho, aby boli za účelom podpory a operácií PLA sprístupnené civilné počítače a iné vybavenie. Tiež pri svojich bežných vojenských operáciách používa zamestnancov z akademickej pôdy a informačne technologického priemyslu. Títo sú trénovaní na podporu PLA vedením široko škálových útokov na siete nepriateľa. Takúto kombináciu civilných a vojenských jednotiek bolo možné vidieť už v Maovej doktríne *"People's War"*. Takisto je to v súlade s Deng Xiaopingovým *"jun min jie he"*, čo znamená *"kombinovať civilov a armádu"* [124].

[121] Ibid
[122] PERRY, William G. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *The Center for Security Policy* [online]. (28) [cit. 2015-05-05]. Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2007-10-China%20Paper%20Final%20Draft%20%282%29.pdf
[123]PERRY, William G. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *The Center for Security Policy* [online]. (28) [cit. 2015-05-05]. Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2007-10-China%20Paper%20Final%20Draft%20%282%29.pdf
[124] Ibid

3. Reakcia USA na čínsku kybernetickú hrozbu

Spojené štáty americké prikladajú čínskej kybernetickej hrozbe nemalú dôležitosť a snažia sa nájsť spôsoby, ako proti nej bojovať. Sám prezident Obama už od svojho príchodu do Bieleho domu v roku 2009 o ňu prejavuje značný záujem. Okrem kybernetických incidentov, z ktorých je mnoho spomenutých v predchádzajúcej kapitole, k tomu mohol prispieť aj fakt, že v predvolebnom období údajne utrpeli jeho kampaňové počítače útok, ktorý mal pochádzať práve z Číny.[125]

V nasledujúcej kapitole rozoberiem spôsoby, akými USA reagujú na čínsku vojenskú a ekonomickú kybernetickú hrozbu.

3.1. Vojenská hrozba

Čínske kapacity pre *„cyberwarfare“* sú rozhodne jedným z dôvodov, ktoré podnietili USA k založeniu nových inštitúcií na posilnenie svojich obranných aj útočných schopností v kybernetickom priestore. Konkrétne tu hovoríme o otvorení *„US Cyber Command“* a vzniku pozície *"kybernetického cára"*.[126]

„U.S. Cyber Command (USCYBERCOM alebo CYBERCOM)“ bolo založené v roku 2009 na príkaz *„Department of Defense (DOD)“*. Je podriadené *„U.S. Strategic Command (USSTRATCOM)“*, ktoré je globálnym synchronizátorom operácií armády Spojených štátov v kybernetickom priestore.[127] Misiou CYBERCOMu je plánovať, koordinovať, integrovať, synchronizovať a prevádzkovať aktivity s cieľom riadenia operácií a obrany špecifikovaných informačných sietí *„US Department of Defense“* a pripraviť sa a na príkaz vykonávať široké spektrum vojenských operácií v kybernetickom priestore za účelom umožnenia jednania

[125] SPADE, JAYSON M. UNITED STATES ARMY. *CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. 2012. Dostupné z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[126] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[127] US DEPARTMENT OF DEFENSE. 2010. *U.S. Cyber Command Fact Sheet*. Dostupné také z: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

vo všetkých doménach, zaistenie slobody konať v kybernetickom priestore pre Spojené štáty a ich spojencov a znemožnenie toho istého pre ich nepriateľov.[128] USCYBERCOM koordinuje služobné prvky každej vetvy armády zahŕňajúc *„Army Forces Cyber Command"* (ARFORCYBER); *„24th USAF"*; *„Fleet Cyber Command"* (FLTCYBERCOM); *„Marine Forces Cyber Command"* (MARFORCYBER) a *„U.S. Coast Guard Cyber Command"*.[129]

Spojené štáty na prevádzkovaní USCYBERCOMu skutočne nešetria. Bolo očakávané, že počet jeho pracovných síl za vlády prezidenta Obamu od roku 2014 do 2016 vzrastie až o 500%. V roku 2013 naň tiež *„US Department of Defense"* vyčlenilo extra 8 miliónov, a to ja napriek výrazným rozpočtovým škrtom.[130]

Pozícia *„Cyber Czar"* alebo odbornejšie *„Cyber-Security Coordinator"* v Bielom dome bola ustanovená v roku 2009 na základe *„Cyberspace Policy Review"*.[131] Do tejto funkcie bol Barackom Obamom menovaný Howard Schmidt, ktorý v nej zotrval do roku 2012.[132] Aktuálne ním je Michael Daniel, ktorý predtým slúžil ako *„Chief of the Intelligence Branch"* v „*National Security Division"*.[133]

Čínska kybernetická hrozba sa odrazila aj v niektorých strategických dokumentoch Spojených štátov. Konkrétne sa budem zaoberať *„Department of Defense Cyber Strategy"* a *„National Security Strategy"* z roku 2015.

Národná bezpečnostná stratégia USA z roku 2015 považuje kybernetické útoky za jednu z hlavných hrozieb bezpečnosti Spojených štátov. Konkrétne o Číne sa súvisiac s kybernetickou bezpečnosťou v Stratégii píše, že Spojené štáty podniknú kroky potrebné

[128] US DEPARTMENT OF DEFENSE. 2010. *U.S. Cyber Command Fact Sheet*. Dostupné také z: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

[129] Ibid

[130] TURNER, Oliver. 2014. *American images of China: identity, power, policy*. 1. London: Routledge. ISBN 9780415659550.

[131] SOOD, Aditya K. a Richard ENBODY. 2014. U.S. MILITARY DEFENSE SYSTEMS: THE ANATOMY OF CYBER ESPIONAGE BY CHINESE HACKERS. *Georgetown journal of International Affairs* [online]. [cit. 2015-05-05]. Dostupné z: http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/

[132] Ibid

[133] White House Profile: Michael Daniel Special Assistant to the President and Cybersecurity Coordinator. *The White House Blog* [online]. [cit. 2015-05-09]. Dostupné z: https://www.whitehouse.gov/blog/author/Michael%20Daniel

na ochranu svojich podnikov a sietí proti kybernetickým krádežiam obchodných tajomstiev na komerčné účely, či už súkromnými aktérmi alebo čínskou vládou.[134]

Čína ako kybernetická bezpečnostná hrozba sa odrazila aj v kybernetickej stratégii *„Department of Defense“* z apríla 2015. *„DOD Cyber Startegy“* zaraďuje medzi kľúčové kybernetické hrozby pre USA fakt, že štáty ako Čína, Severná Kórea či Rusko masívne investovali do svojich kybernetických kapacít a stratégií, čo im dáva prostriedky na to, aby ohrozili bezpečnosť a záujmy USA. Konkrétne pri Číne *„DOD Cyber Startegy“* zdôrazňuje problém krádeží duševného vlastníctva za účelom pomôcť čínskym spoločnostiam a podkopať konkurencieschopnosť USA.

Za svoj cieľ v tejto oblasti si *„Department of Defense“* stanovilo posilniť dialóg s Čínou za účelom posilnenia strategickej stability. Dané dialógy majú byť realizované v rámci *„U.S.-China Defense Consultative Talks“* a súvisiacich dialógov ako je *„Cyber Working Group“*. Prostredníctvom nich má DOD v záujme zlepšiť vzájomné porozumenie medzi štátmi, transparentnosť vojenských doktrín, stanoviť politiku, misie a role v kybernetickom priestore a redukovať nedorozumenia, ktoré môžu spôsobiť nestabilitu. DOD sa tiež chystá zvyšovať povedomie o čínskou kybernetickou krádežou duševného vlastníctva, obchodných tajomstiev a dôverných podnikateľských informácií.[135]

3.2. Ekonomická hrozba

Podarilo sa mi identifikovať niekoľko spôsobov, ktorými Spojené štáty reagujú na čínsku kybernetickú hrozbu ekonomického a súčasne s ňou aj vojenského charakteru. Medzi ne patria: vzájomný dialóg medzi USA a Čínou realizovaný v rámci pracovných skupín, stretnutí na úrovni hláv štátov a pokusov o nadviazanie spolupráce v konkrétnych prípadoch; multilateralizácia otázky kybernetickej bezpečnosti; *„naming and shaming“*; ekonomické sankcie; snaha o podnietenie amerických podnikov k vyššiemu záujmu o ochranu vlastného duševného vlastníctva; spolupráca amerických firiem s Vládou Spojených štátov.

Asi najjednoduchším a najzákladnejším spôsobom, akým by Spojené štáty mohli reagovať a reagujú na čínsku kybernetickú špionáž a krádeže dát je takzvaná metóda *„naming*

[134] THE WHITE HOUSE. 2015. *National Security Strategy*. Dostupné také z: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

[135] THE DEPARTMENT OF DEFENSE. 2015. *The DoD Cyber Strategy*. Dostupné také z: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.p

and shaming", ktorá elementárne spočíva vo verejnom označení *„hriešnika"* dúfajúc, že bude zahanbený a už viac vo svojej aktivite nebude pokračovať. Implementácia tejto taktiky je naozaj jednoduchá.[136] Obamova administratíva opakovane a verejne nazvala Čínu svojím hlavným nepriateľom v oblasti kybernetickej špionáže, zdôrazňujúc agresívnu ekonomickú kybernetickú špionáž proti hospodárskej a kritickej infraštruktúre Spojených štátov.[137] Medzi príklady takéhoto *„naming and shaming"* patria napríklad správy Mandiantu o APT a ATP1. Snáď najznámejším z prípadov *„naming and shaming"* sa stal v roku 2014, kedy „*U.S. Justice Department"* obvinilo piatich čínskych vojenských úradníkov z kybernetickej krádeže v piatich z amerických korporácií a hlavnej medzinárodnej odborovej únii.[138] Toto obvinenie nadobudlo v Číne veľký protiamerický ohlas. Viedlo ku znevýhodňovaniu amerických firiem v Číne a k intenzívnym mediálnym kampaniam naprieč Čínou kritizujúcim aktivitu Spojených štátov amerických v kybernetickom priestore. Tieto označili domáci pokrok a inovácie za kľúč ku zlepšeniu kybernetickej bezpečnosti krajiny a zníženiu závislosti Číny na zahraničných technológiách.[139] Tento prípad ako aj mnohé iné dokazuje, že metóda *„naming and shaming"* bohužiaľ nevykazuje nejaké prevratné výsledky. Vinník často svoju chybu neprizná, ten, čo obviňuje sa stáva terčom kritiky, a nie je dokázané, že by sa na jej základe špionáž zmiernila, v niektorých prípadoch sa dokonca zintenzívňuje.[140]

Okrem metódy *„naming and shaming"* sa Spojené štáty snažia problém ekonomickej špionáže adresovať predovšetkým pomocou udržiavania dialógu a vzájomnej spolupráce s Čínou v oblasti kybernetickej bezpečnosti. Ako povedal James Mulvenon[141]: *„Určite, stále potrebujeme mať dialóg a stále a nimi potrebujeme jednať, a stále s nimi potrebujeme hovoriť*

---

[136] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[137] 4 ways US can boost cyber security. In: *The Christian Science Monitor* [online]. n.d. [cit. 2015-04-25]. Dostupné z:http://www.csmonitor.com/Commentary/Opinion/2013/0409/4-ways-US-can-boost-cyber-security/Start-where-countries-agree

[138] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[139] JONG - CHEN, Jing De. 2014. U.S.-CHINA CYBERSECURITY RELATIONS: UNDERSTANDING CHINA'S CURRENT ENVIRONMENT.*Georgetown Journal of International Affairs* [online]. [cit. 2015-05-05]. Dostupné z: http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/

[140] GADY, Franz Stefan. He Axiom Report: Cybersecurity and Its Impact on China-US Relations. In: *East West Institute*[online]. 2014 [cit. 2015-04-25]. Dostupné z: http://www.ewi.info/idea/axiom-report-cybersecurity-and-its-impact-china-us-relations

[141] Vice prezident v „*Defense Group Incorporated's Intelligence Division"* a riaditeľ *„DGI's Center for Intelligence Research and Analysis"*

o kontrole zbraní a kybernetickej kriminalite a spolupráci v oblasti kybernetickej kriminality, a potrebujeme sa vysporiadať so záležitosťami ohľadne internet governance...“[142]

Tento dialóg môže byť realizovanými viacerými spôsobmi. Prvým z nich je na báze stretnutí hláv štátov a iných štátnych predstaviteľov či odborníkov.

V júni roku 2013, sa prezidenti Obama a Xi Jinping stretli na summite s názvom *„Sunnyland“* konajúcom sa v Kalifornii. Jeho cieľom bolo pomocou relatívne neformálnych sedení znížiť vzájomnú nedôveru medzi Čínou a USA. Na programe summitu boli problémy ako námorné a obchodné otázky či iránsky a severo – kórejský nukleárny program. Kybernetická bezpečnosť stála ako najdôležitejšia téma na samom vrchole agendy. Pre USA bolo toto stretnutie pokračovaním dlhodobého snaženia o dotlačenie Pekingu k zníženiu počtu kybernetických útokov proti USA.[143] Efekt tohto stretnutia bol však veľmi diskutabilný, keďže jeden deň po jeho skončení sa Edward Snowden v Hong Kongu odhalil ako zdroj informácií o programe dohľadu USA nad telekomunikačnými a internetovými dátami, ktorému sa budem venovať trochu neskôr.[144]

Hlavy Číny a USA sa tiež stretli v belgickom Hágu v marci 2014 počas summitu o jadrovej bezpečnosti. Prediskutovali široké spektrum záležitostí od Severnej Kórei, cez námorné záležitosti Číny až po kybernetickú bezpečnosť. Barack Obama zdôrazňoval nevyhnutnosť bližšej spolupráce v rámci problematiky kybernetickej bezpečnosti. Riešila sa tam takisto správa New York Times o tom, že NSA hackovala servery čínskej firmy Huawei. Prezident Obama prezidenta Xiho uistil o tom, že USA to nerobili s cieľom získania ekonomických výhod.[145]

Téme kybernetickej bezpečnosti sa tiež americký a čínsky prezident venovali na summite Asia-Pacific Economic Cooperation (APEC) Economic Leaders' Meeting v Pekingu v novembri 2014. Táto téma tam však bola dotknutá iba okrajovo. Dôvodov preto môže byť niekoľko. Prvým je, že hlavy štátov sa nepohodli na konkrétnej téme. Xi Jinping chcel

[142] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[143] SEGAL, Adam M. Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis* [online]. 2014, č. 4 [cit. 2015-04-25]. Dostupné z: http://www.tandfonline.com/doi/pdf/10.1080/09700161.2014.918447

[144] Ibid

[145] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

rozprávať o kybernetickom terorizme, Barack Obama o dôležitosti ochrany duševného vlastníctva. Druhým dôvodom môže byť napätie vo vzťahu spôsobené už spomínaným obvinením čínskych vojenských úradníkov zo špionáže.[146] Na tomto summite sa im však podarilo vyjednať dohodu o obchode s informačnými technológiami.[147]

Ďalším zo spôsobov riešenia problému ekonomickej kybernetickej špionáže je snaha Spojených štátov o vytvorenie mechanizmov umožňujúcich dialóg v oblasti kybernetickej bezpečnosti. Táto snaha prispela k založeniu *„U.S.-China Cyber Working Group"* v roku 2013, a to v rámci ekonomického a strategického dialógu medzi Čínou a USA a za účelom bilaterálneho dialógu o kybernetickej bezpečnosti.[148] Čína však svoju účasť v nej zrušila v máji roku 2014 po tom, čo „*U.S. Justice Department"* obvinilo spomínaných piatich čínskych vojenských úradníkov z kybernetickej krádeže v amerických korporáciách. [149]

Snahu o zlepšenie vzájomného vzťahu v kybernetickej oblasti môžeme vidieť aj na konkrétnych pokusoch o nadviazanie spolupráce v reálnych prípadoch. Jedným z nich bol aj prípad Sony Pictured Entertainment. V novembri 2014 bola spoločnosť Sony Pictured Entertainment zasiahnutá kybernetickým útokom, ktorý zmrzačil jej siete a ukradol veľké množstvo osobných aj obchodných dát. V decembri FBI identifikovala Severnú Kóreu ako vinníka útoku. Niektorí analytici tvrdia, že na útoku mohla mať svoj podiel aj Čína, no z diplomatických dôvodov nebolo vynesené verejné obvinenie. Naopak, administratíva USA požiadala Čínu o spoluprácu, predovšetkým v rámci zdieľania informácií a blokovania budúcich kórejských kybernetických útokov.[150]

„U.S.-China Economic and Security Review Commission" nepredpokladá, že by Čína túto ponuku na spoluprácu prijala, a to zakladajúc na troch faktoch:

Prvým z nich je už vyššie spomínané obvinenie čínskych vojenských úradníkov zo špionáže z mája 2014.[151] Druhým dôvodom je to, že podľa Číny nie je dostatočne potvrdené, že za

[146] APEC 2014: All Quiet on the Cyber Front? 2014. GADY, Franz-Stefan. *China - US Focus* [online]. [cit. 2015-05-09]. Dostupné z: http://www.chinausfocus.com/peace-security/apec-2014-all-quiet-on-the-cyber-front/
[147] MORRISON, Wayne M. 2015. China-U.S. Trade Issues. *Congressional Research Service* [online]. [cit. 2015-05-09]. Dostupné z: https://fas.org/sgp/crs/row/RL33536.pdf
[148] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[149] Ibid
[150] *China's Position on the Sony Attack: Implications for the U.S. Response: U.S.-China Economic and Security Review Commission Staff Report*. 2015.
[151] Ibid

týmto útokom skutočne stojí Severná Kórea. Tretím dôvodom je, že Čína doma aktívne cenzuruje informácie o tomto kybernetickom útoku.[152]

Z predchádzajúceho textu môžeme usúdiť, že USA sa nesnažia Čínu len z kybernetických útokov priamo obviňovať a donútiť k tomu, aby s nimi prestala. Kybernetickú špionáž sa pokúšajú redukovať tiež prostredníctvom zlepšenia ich vzťahu s Čínou, ktorý by mal byť vybudovaný na vzájomnom porozumení. Tiež sa s Čínou snažia spolupracovať v otázkach kybernetickej bezpečnosti a dosiahnuť vzájomné porozumenie tiež v tejto oblasti.

Táto námaha, ktorú USA vynakladajú, bola značne poškodená aférou Snowden. Edward Snowden zapríčinil problém, ktorý stál Washington naozaj veľa diplomatického úsilia.

Edward Snowden je bývalým kontraktorom Národnej bezpečnostnej agentúry, ktorý v roku 2013 v Hong Kongu poskytol reportérovi britského denníka The Guardian, Glennovi Greenwaldovi[153], utajované materiály obsahujúce informácie o tom, že NSA nelegálne sledovala metadáta miliónov ľudí v Spojených štátoch a Európe, a to nielen v otázkach národnej bezpečnosti. Operácie NSA mali byť tiež zamerané na diplomatickú a ekonomickú špionáž. Tieto dokumenty okrem iného obsahovali detailné informácie o takzvanom *„globálnom programe dohľadu“*, ktorý NSA realizovala spolu s britskou, kanadskou a austrálskou spravodajskou službou, a ktorý okrem iného sledoval aj Čínu. Ako prvý bol v médiách spomenutý program nazvaný PRISM. V jeho rámci mali byť sprístupňované dáta spoločností, ktorými boli napríklad Google, Facebook, Skype, YouTube či Yahoo[154]. Podľa Snowdena NSA disponuje vybavením schopným zachytiť e-maily, telefónne hovory a údaje o nich či heslá kreditných kariet.

Prvý článok o téme Snowden bol zverejný v britskom denníku the Guardian. Neskôr nasledovali nemecký Der Spiegel, Washigton Post, New York Times a iné.[155] Snowden

---

[152] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION*. Washington DC, 2014. Dostupné z: http://www.uscc.gov

[152] JONG - CHEN, Jing De. 2014. U.S.-CHINA CYBERSECURITY RELATIONS: UNDERSTANDING CHINA'S CURRENT ENVIRONMENT.*Georgetown Journal of International Affairs* [online]. [cit. 2015-05-05]. Dostupné z: http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/

[153] GREENWALD, Glen. 2014. *No place to hide*. London: Penguin Books. ISBN 9780241146699.

[154] Ibid

[155] Aféra Snowden: Ako zmenila Európu? 2014. *EurActiv 2014*[online]. [cit. 2014-09-05]. Dostupné z: http://www.euractiv.sk/parlamentny-spravodaj-000461/zoznam_liniek/afera-snowden-ako-zmenila-europu-000332

odhalil svoju identitu na vlastnú žiadosť a v súčasnosti žije pod dočasným azylom v Rusku. V Spojených štátoch je trestne stíhaný.[156]

Obama po tomto incidente na obhajobu USA zdôraznil rozdiel medzi získavaním spravodajského materiálu na vojenské a politické účely a priemyselnou špionážou. Pre reportérku Charlie Rose povedal:[157]

„...Každá krajina na svete, malá či veľká, sa angažuje v získavaní spravodajského materiálu...Je veľký rozdiel medzi tým, keď chce Čína prísť na to, ako môžu zistiť, o čom sa bavím pri stretnutiach s Japoncami, čo je bežné...a hackerom priamo napojeným na čínsku vládu alebo čínsku armádu, ktorý sa vláme do softwarového systému Applu, aby zistil, či môže získať návrhy posledného produktu. To je krádež. A to my nemôžeme tolerovať. "[158]

Je však nutné poznamenať, že tento rozdiel je, a to aj v prípade získavania spravodajského materiálu pre vládu USA, často ťažko rozpoznateľný.[159]

Po Snowdenovom odhalení Peking nazval USA *„skutočným hackerským impériom"* a vyžadoval medzinárodnú spoluprácu v záležitosti dohľadu a USA trochu zmiernilo svoj dovtedajší diplomatický nátlak na Čínu. Hoci *„US National Security Advisor"* Susan Rice v novembri 2013 varovala, že záležitosť kybernetickej špionáže dokáže podkopať vzájomné obchodné vzťahy Číny a USA, *„Treasury Secretary"* Jacob Lew vo svojich *„public talking points"* v Pekingu v ten istý mesiac kybernetickú bezpečnosť nespomenul.[160]

No napriek tomu, že pozícia Washingtonu bola po tomto incidente výrazne oslabená, mali USA i naďalej v zámere riešiť s Pekingom otázky kybernetickej špionáže, a to na základe bilaterálnej *„U.S.-China Cyber Working Group"* a cez multilaterálne fóra, ako napríklad *„ASEAN Regional Forum"*.[161]

---

[156] Aféra Snowden.2014. *Europska Unia* [online]. [cit. 2014-09-05]. Dostupné z: http://www.europskaunia.sk/afera-snowden

[157] SEGAL, Adam M. 2014. Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis* [online]. (4) [cit. 2015-05-05]. Dostupné z: http://www.tandfonline.com/doi/pdf/10.1080/09700161.2014.918447#.VUjrufntmko

[158] SEGAL, Adam M. 2014. Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis* [online]. (4) [cit. 2015-05-05]. Dostupné z: http://www.tandfonline.com/doi/pdf/10.1080/09700161.2014.918447#.VUjrufntmko

[159] Ibid

[160] SEGAL, Adam M. 2014. Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis* [online]. (4) [cit. 2015-05-05]. Dostupné z: http://www.tandfonline.com/doi/pdf/10.1080/09700161.2014.918447#.VUjrufntmko

[161] Ibid

Hovoriac o multilaterálnych fórach, Spojené štáty americké určite nie sú jedinou obeťou kybernetickej špionáže a takisto Čína nie je jej jediným pôvodcom. Preto USA považujú za vhodné proti tomuto problému bojovať tvorbou multilaterálnych koalícií, ktoré sa už v mnohých iných prípadoch osvedčili.[162]

Jedným z úsilí Spojených štátov je presadiť zdieľanie informácií na medzinárodnej úrovni. Ďalšou z možností je tvorba partnerstiev. USA sa momentálne angažujú v nasledujúcich prebiehajúcich jednaniach: *„Trans-Pacific Partnership"* a *„Trans-Atlantic Trade and Investment Partnership".*[163] *„Trans-Pacific Partnership"* je medzinárodnou investičnou a regulatívnou zmluvou. Jej vyjednávania prebiehajú od roku 2005 a zúčastňujú sa na nich nasledujúce krajiny: Austrália, Brunej, Kanada, Chile, Japonsko, Malajzia, Mexiko, Nový Zéland, Peru, Singapur, Spojené štáty americké a Vietnam.[164] *„Trans-Atlantic Trade and Investment Partnership"* je návrh dohody o voľnom obchode medzi Spojenými štátmi a Európskou úniou[165]. Tieto zmluvy majú prispieť k zvýšeniu štandardov ochrany duševného vlastníctva a rozšíriť dimenzie spolupráce a zdieľania informácií.[166]

Okrem dialógu sa USA proti kybernetickej ekonomickej špionáži snažia bojovať aj prostredníctvom sankcií uvaľovaných na jej pôvodcov. Tento spôsob je nový, pochádzajúci z roku 2015. Prvého apríla 2015 USA spustili nový program, ktorý má za cieľ zastrašiť a finančne napádať cudzie strany, ktoré sa angažujú, podporujú alebo profitujú zo *"significant malicious cyber-enabled activities."*[167] Vyhlásiac národnú pohotovosť, prezident Barack Obama vydal vládny príkaz, ktorý poveril *„Secretary of the Treasury"*, aby po konzultácii

---

[162] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[163] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[164] Trans-Pacific Partnership Agreement. *Electronic Frontier Foundation: Defending your rights in the digital world* [online]. [cit. 2015-05-10]. Dostupné z: https://www.eff.org/issues/tpp

[165] Transatlantic Trade and Investment Partnership. *Office of the United States Trade Representative* [online]. [cit. 2015-05-10]. Dostupné z: https://ustr.gov/ttip

[166] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[167] SIDLEY. *New U.S. Sanctions Program Targets Malicious Foreign-Origin Cyber Activities: Sanctions Update*. 2015. Dostupné z: http://www.sidley.com/~/media/update%20pdfs/20150402%20sanctions%20update.pdf

s *„Attorney General*“ a *„Secretary of State“* označila ako *„Specially Designated Nationals“* a *„Blocked Persons (SDNs)“* všetkých kybernetických aktérov, ktorí nezanedbateľne ohrozujú národnú bezpečnosť, zahraničnú politiku, hospodárske zdravie či finančnú stabilitu Spojených štátov. K spusteniu tohto programu došlo ako reakcia na kybernetické útoky zo štátov ako Čína, Severná Kórea či Rusko.[168] *"Obamova administratíva to začína brať skutočne vážne. Tento príkaz uplatňuje ekonomickú moc Spojených štátov proti ľuďom, ktorí nás slepo okrádajú a dostávajú nás do nebezpečenstva.,"*[169] povedal Joel Brenner, ktorý viedol U.S. counterintelligence počas druhého prezidentského obdobia Georga W. Busha.[170]

Dôležitá nie je len aktivita, ktorú USA vykonáva navonok voči ostatným štátom. Potrebné sú tiež opatrenia vo vnútri USA. Je žiaduce, aby si samotné spoločnosti v Spojených štátoch chránili svoje duševné vlastníctvo, aby určili, čo ním je, aké je to cenné, čo by ho mohlo ohroziť, a aby si na to dávali pozor. Preto sa v USA snažia presadiť spoluprácu súkromného sektoru s Vládou Spojených štátov v rámci zdieľania informácií. Vláda môže vďaka svojím mnohým zdrojom pomôcť spoločnostiam identifikovať zdroje hrozieb, použité technológie a spôsoby, ako sa proti nim brániť.[171]

Spojené štáty majú tiež v zámere urobiť krádež duševného vlastníctva amerických spoločností pre zahraničné firmy nevýhodnou – chcú dosiahnuť, aby sa im už viac nevyplatila, aby náklady na ňu prevýšili zisky. Prvým krokom v tomto snažení má byť zdôraznenie dôležitosti prístupu na americký trh pre tie firmy, ktoré chcú byť medzinárodnými obchodnými lídrami. Komisia navrhuje, aby sa toto snaženie realizovalo napríklad pomocou poskytnutia väčšieho množstva zdrojov pre FBI či daním *„Treasury“* právomoc na to, aby mohla dané firmy vylúčiť z bankového systému. Zvýšenie nákladov na kybernetickú špionáž chce „*U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION“* realizovať tiež za pomoci vytvorenia komunity v Číne, ktorá je špionážnym úsilím čínskej vlády, s ktorým nemá nič spoločné, poškodzovaná. Do tejto komunity by patrili univerzity a spoločnosti, ktoré sú s kybernetickou

[168] SIDLEY. *New U.S. Sanctions Program Targets Malicious Foreign-Origin Cyber Activities: Sanctions Update*. 2015. Dostupné z: http://www.sidley.com/~/media/update%20pdfs/20150402%20sanctions%20update.pdf

[169] U.S. targets overseas cyber attackers with sanctions program. In: MASON, Jeff a Andrea SHALAL. *Reuters.com* [online]. 2015 [cit. 2015-04-26]. Dostupné z: http://www.reuters.com/article/2015/04/01/us-usa-cybersecurity-idUSKBN0MS4DZ20150401

[170] Ibid

[171] MOHAN, C. Raja. *US-China Cyber Talks: internet security in the global economy*. 2013. Dostupné z: http://hdl.handle.net/10220/13340

špionážou spájané ako členovia aparátu štátnej bezpečnosti, vojenskí kontraktori či tvorcovia malware. Takéto osoby sa potom dostávajú na čierne listiny, nedostanú víza do Spojených štátov, profesori inkriminovaných univerzít nedostanú štipendium, nemôžu sa vrátiť do USA.

4. Medzery v reakcii USA na čínsku kybernetickú hrozbu

Na základe predchádzajúceho textu a podrobného štúdia problematiky sa mi podarilo identifikovať niekoľko medzier a nezrovnalostí v stratégii Spojených štátov amerických v boji proti čínskej kybernetickej hrozbe.

V predchádzajúcom texte sa venujem dialógu medzi USA a Čínou. Tento dialóg prebieha na báze stretnutí hláv štátov a iných štátnych predstaviteľov a vo forme komunikácie v rámci rôznych fór a pracovných skupín. Identifikovala som dva problémy, ktoré brzdia túto komunikáciu. Prvým z nich môže byť rozdielna terminológia na strane Číny a USA. Totižto, medzi týmito dvoma štátmi neexistuje jednotná definícia kľúčových pojmov z oblasti kybernetickej bezpečnosti, a teda ešte aj tak základné termíny ako sú informácia alebo kybernetický útok sú používané inak americkou a inak čínsku vládou.[172] Tento dialóg a spolupráca sú tiež značne komplikované kauzami ako Snowden, ktoré odhaľujú praktiky USA a dovoľujú Číne myslieť si, že nerobí nič nesprávne, pretože USA konajú to isté. Číňania veria, že USA pri každej príležitosti napádajú ich siete.[173] Tým pádom je ťažké nechcieť od nich, aby robili to isté.

Ďalej v práci píšem o snahe podporovať spoluprácu amerických firiem a vlády v rámci ochrany proti kybernetickým útokom. Problémom v tejto oblasti môže byť to, že firmy často nechcú spolupracovať alebo komunikovať. Majú strach, že zverejnenie toho, že ich duševné vlastníctvo bolo ukradnuté, im uškodí. Napríklad, nechcú, aby sa o tomto probléme dozvedela Wall Street, pretože by sa to mohlo veľmi negatívne odraziť na hodnote akcií ich spoločnosti.[174]

Zvýšená ochrana vlastného kybernetického majetku je zasa nákladná a hlavne malým a stredným podnikom sa finančne neoplatí. Jedným z takýchto opatrení nevýhodných pre malé a stredné podniky je to, že podľa odporúčaní *„US – China economic and security*

[172]MOHAN, C. Raja. *US-China Cyber Talks: internet security in the global economy*. 2013. Dostupné z: http://hdl.handle.net/10220/13340
[173] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf
[174] Ibid

review commission" by si mali vo firme zriadiť veľkú entitu zaoberajúcu sa radením ohľadne kybernetickej bezpečnosti.[175]

V predošlem texte sa tiež venujem praktike zvanej *„naming and shaming"*, ktorá v jednoduchosti znamená verejné označenie vinníka a dúfanie, že bude zahanbený. Medzerou, na ktorú narážam, nie je samotné *„naming and shaming"*, ale prípadná snaha o sankcionovanie vinníka po tom, čo je *„named and shamed".* Ak v minulosti po *„naming"* prišiel zámer uvaliť na *„vinníka"* trest, vznikalo mnoho ťažko riešiteľných otázok ohľadne implementácie a vhodnosti sankcie[176]. Vzhľadom na rozbehnutie nového sankčného programu USA v apríli tohto roku sa situácia možno zlepší.[177]

Ďalším z problémov, ktorý sa mi podarilo identifikovať, je právne uchopenie problematiky v Spojených štátoch. Totižto, obeť musí po kybernetickom útoku preukázať nielen to, že došlo ku krádeži informácií alebo duševného vlastníctva. V mnohých prípadoch je tiež potreba dokázať materiálnu ujmu, čo znamená, že nie je možné materiálnej ujme zabrániť predtým, než sa stane. Materiálnu ujmu často nie je možné dokázať vôbec a poškodení sa nikdy nedočkajú rekompenzácie.[178]

Tiež je možné, že v Spojených štátoch sa nachádzajú aktéri, ktorí majú vo svojom záujme zveličovanie čínskych kybernetických kapacít, a to v záujme odôvodnenia svojej vlastnej existencie a získania zvýšeného rozpočtu. Medzi takýchto aktérov sa môžu zaraďovať Pentagon, určití politici či spravodajské služby. Títo sú obviňovaní z obdobného správania ako za studenej vojny, čím prispievajú ku konfliktných vzťahom medzi Čínou a Spojenými štátmi.[179]

---

[175] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[176] Ibid

[177] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[178] UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

[179] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

Poslednou z nezrovnalostí, ktoré sa mi podarilo nájsť, je možnosť, že mnohé útoky, za ktoré je Čína obviňovaná, vôbec nie sú realizované z Číny. Totižto, vlastné siete Číny sa zdajú byť nechránené, čo umožňuje iným aktérom realizovať cez ne útoky na USA, pričom Čína sa zdá byť primárnym podozrivým.[180] IT expert Steve Armstrong povedal: *"je príliš jednoduché obviňovať Čínu… V skutočnosti, legitímne štáty vykonávajú svoje útoky cez Čínu. Je veľmi jednoduché to urobiť, tak prečo nie?... Mojou diabolskou myšlienkou je, že niektoré západné vlády to už realizujú.."*[181]

Kybernetickej bezpečnosti je v Čínskej ľudovej republike vo všeobecnosti pripisovaný veľmi malý význam,[182] čo môžeme vidieť hneď na niekoľkých príkladoch. Prvým z nich je už to, že toto slovné spojenie a výzvy, ktoré predstavuje, nie sú čínskymi autoritami detailne definované. Vyhlásenia čínskej vlády v kontexte kybernetickej bezpečnosti väčšinou referujú ku všeobecným pojmom ako nárast používania internetu, rastúca závislosť mnohých národov na aktivitách odohrávaných v kybernetickom priestore, potenciálne hrozby predstavované kybernetickými útokmi či potreba vládneho dohľadu nad internetom.[183] Kybernetická bezpečnosť v Číne takisto nie je dosť legislatívne a inštitucionálne upravená, informačné a bezpečnostné plány a stratégie sú nedostatočné a verejné vzdelávanie v tejto oblasti tiež nie je možné označiť za dostačujúce. Súkromie a dáta sú tam veľmi slabo chránené a medzinárodná spolupráca v oblasti kybernetickej bezpečnosti by bola pre Čínu viac než prínosná[184]. Za problém sa dá považovať tiež to, že mnohé záležitosti týkajúce sa kybernetickej bezpečnosti sú v Pekingu zatláčané do úzadia, pretože vysokí politickí činitelia dávajú prednosť venovaniu sa záležitostiam, ktoré považujú za akútnejšie[185]. Civilný aparát kybernetickej bezpečnosti je formovaný technicky zameranými ľuďmi bez ekonomických či politických znalostí. Politika v oblasti kybernetickej bezpečnosti je teda v Číne veľmi

[180] HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 2001, č. 4 [cit. 2015-04-25]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

[181] Ibid

[182] *China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops held at the University of California, San Diego*. 2012. Dostupné také z: http://igcc.ucsd.edu/assets/001/503541.pdf

[183] SWAINE, Michael D. 2013. Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://carnegieendowment.org/files/CLM42MS.pdf

[184] LINDSAY, Jon. 2012. *China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops held at the University of California, San Diego* [online]. [cit. 2015-05-13].

[185]Ibid

slabo koordinovaná, čo spôsobuje jej stagnáciu[186]. Na základe týchto skutočností môžeme usúdiť, že prevedenie útoku cez Čínu inými štátmi je naozaj dosť možné.

[186]LINDSAY, Jon. 2012. *China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops held at the University of California, San Diego* [online]. [cit. 2015-05-13].

Záver

Cieľom mojej diplomovej práce bolo zodpovedať na nasledujúce otázky: Akú kybernetickú hrozbu predstavuje Čína pre Spojené štáty americké? Ako má nadefinovanú svoju kybernetickú stratégiu? Ako na túto hrozbu reagujú USA a aké sú medzery v ich reakcii?

V prvej kapitole práce som sa zaoberala pojmom *„cyberwarfare“*. Na začiatku som ho definovala, a potom som sa mu venovala v súvislosti s Čínskou ľudovou republikou.

V druhej kapitole som sa venovala kybernetickej hrozbe Číny pre bezpečnosť USA. Na začiatku kapitoly som popísala vzájomný vzťah týchto štátov a naznačila dôvody, prečo majú tieto štáty jeden o druhý záujem, okrem iného tiež v kybernetickej oblasti. Potom som sa zaoberala kybernetickou hrozbou, ktorú Čína predstavuje pre USA. Túto hrozbu som rozdelila na vojenskú a ekonomickú.

V ďalšej kapitole som riešila spôsoby, akými sa USA bránia proti čínskej vojenskej a ekonomickej kybernetickej hrozbe. Pri vojenskej hrozbe som sa venovala vzniku nových inštitúcií a strategických dokumentov. Pri ekonomickej som riešila obviňovanie Číny z kybernetických útokov zo strany USA, vzájomný dialóg a spoluprácu v kybernetickej oblasti, ekonomické sankcie a opatrenia prijaté vo vnútri Spojených štátov.

V štvrtej kapitole som sa pokúsila určiť medzery v jednotlivých spôsoboch, ktorými sa Spojené štáty bránia proti čínskej kybernetickej hrozbe a nezrovnalosti v ich stratégii.

Svoju prácu som založila na fakte, že všeobecná definícia *„cyberwarfare“* a jeho oddelenie od ekonomickej špionáže v čínskom prípade celkom neplatí. Na výkone aktivít považovaných za súčasť *„cyberwarfare“* sa tam v súlade s čínskou doktrínou *„cyberwarfare“* okrem PLA významne podieľa aj súkromný sektor – IT spoločnosti, univerzity či civilní hackeri. V rámci snahy o koordinovaný vývoj hospodárstva a národnej obrany sa kybernetické útoky používajú na podporu armády i čínskeho hospodárstva. Útočí sa na komerčné ciele, ktoré majú nejakú spojitosť s vojenskou technológiou.

Čína v kybernetickom priestore pre USA predstavuje vojenskú a ekonomickú hrozbu. Svojou ekonomickou špionážou systematicky rozkladá konkurencieschopnosť firiem USA a spôsobuje USA značné finančné škody. Medzi najväčšie hrozby ekonomického charakteru patria tímy ATP, ktoré majú pracovať pod čínskou armádou a darí sa im ukradnúť najväčšie množstvo dát. Čo sa týka vojenskej hrozby, tou je predovšetkým to, že Čína je na nízke

náklady schopná paralyzovať vojenské vedenie a kontrolu a kritickú infraštruktúru Spojených štátov. Doposiaľ bolo zaznamenaných niekoľko útokov tohto charakteru. Takéto aktivity sú v USA považované za súčasť programu *„kybernetickej rozviedky“,* ktorý Číne slúži na testovanie počítačových sietí amerických vládnych agentúr a súkromných organizácií, nachádzanie ich slabých miest, objavenie vzorcov v komunikácii vládnych a súkromných organizácií a získavanie tajných informácií.

V práci sa mi podarilo identifikovať niekoľko spôsobov, ktorými Spojené štáty reagujú na čínsku kybernetickú hrozbu ekonomického aj vojenského charakteru. Na vojenskú hrozbu Spojené štáty reagujú tvorbou nových inštitúcií a zahŕňaním čínskej kybernetickej hrozby do strategických dokumentov, menovite „*CYBERCOM“ a „Cyber Czar“,* čo sa týka inštitúcií a *„Department of Defense Cyber Strategy“* a *„National Security Strategy“* hovoriac o dokumentoch. Ako reakciu na ekonomickú hrozbu, USA realizujú metódu *„naming and shaming“*, vedú s Čínou dialóg na báze stretnutí hláv štátov či pracovných skupín, pokúšajú sa o nadviazanie spolupráce v konkrétnych prípadoch v oblasti kybernetickej bezpečnosti, snažia sa o podnietenie amerických podnikov k vyššiemu záujmu o ochranu vlastného duševného vlastníctva a k spolupráci amerických firiem s Vládou Spojených štátov. Najnovšie bol zavedený aj program ekonomických sankcií.

Tiež sa mi podarilo nájsť niekoľko medzier v reakcii USA na čínsku kybernetickú hrozbu. Neexistencia jednotnej definície kľúčových pojmov z oblasti kybernetickej bezpečnosti a kauzy ako Snowden alebo obvinenie čínskych úradníkov o špionáže negatívne ovplyvňujú dialóg a vzájomnú spoluprácu. Americké firmy sú tiež často neochotné spolupracovať s vládou a zavádzať niektoré opatrenia na zvýšenie ochrany svojho majetku. Právne uchopenie problematiky kybernetickej krádeže v USA nedovoľuje v prípade krádeže dát zabrániť materiálnej ujme skôr, než k nej dôjde. Donedávna bolo problematické tiež určiť výšku a rozsah sankcií, ktoré mohli byť uvalené po *„naming and shaming“*. Často je problematické jasne určiť, že útoky skutočne pochádzajú z Číny.

Summary

In cyber space, China represents economic and military threat for US. It is systematically ruining competitiveness of its companies causing their significant financial loss. Among the biggest economic threat belong ATP teams which are supposed to work on behalf of the Chinese army and able to steal the biggest amount of data. Military threat is predominantly represented by Chinese ability to paralyze US military conduct and control, and US critical infrastructure at low cost. So far, several attacks of this character have been recorded.

I was able to identify several ways of the US reaction on the Chinese economic and military cyber threat. The reaction on the military threat is represented by establishing new institution and handling the Chinese cyber threat in the US strategic documents. On the economic threat, US react with several ways: *"naming and shaming"* method, bilateral and multilateral dialog, cooperation on concrete cyber security cases, establishing cooperation of the US Government with US companies in order to fight against cyber espionage, increasing protection of intellectual property in US companies, and imposing of sanctions.

I found several gaps in the US reaction. The absence of uniform definition of cyber security terms and causes like Snowden have negative effect on the US – Chinese dialog and cooperation. US companies are often unwilling to cooperate with the Government and to impose some measures to protect their property. Often it is difficult to prove that cyber attacks really originate from China. Legislative measures in USA dealing with cyber theft are insufficient.

Bibliografia

Dokumenty

IOSCO RESEARCH DEPARTMENT AND WORLDS FEDERATION OF EXCHANGES. 2013. *Cyber-crime, securities markets and systemic risk* [online]. [cit. 2015-05-13]. Dostupné také z: http://www.csrc.gov.cn/pub/csrc_en/affairs/AffairsIOSCO/201307/W021307195219604684 95.pdf

MANDIANT. *APT1 Exposing One of China's Cyber Espionage Units*. 2013. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

MANDIANT. 2010. *The Advanced Persistent Threat*. Dostupné také z: https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf

THE WHITE HOUSE. 2015. *National Security Strategy*. Dostupné také z: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. 2014. *2014 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION* [online]. [cit. 2015-05-13]. Dostupné také z: http://www.uscc.gov

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. 2006. *2006 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION* [online]. [cit. 2015-05-13]. Dostupné také z: http://www.uscc.gov

US Departament of Defense.2015.*The DoD Cyber Strategy*. Dostupné také z: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.p

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *U.S.-CHINA CYBERSECURITY ISSUES: Roundtable*. Washington DC, 2013. Dostupné z: http://origin.www.uscc.gov/sites/default/files/transcripts/USCC%20Roundtable%20Transcript%20-%20July%2011%202013.pdf

US DEPARTMENT OF DEFENSE. 2010. *U.S. Cyber Command Fact Sheet*. Dostupné také z: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. 2015. *China's Position on the Sony Attack: Implications for the U.S. Response: Staff Report* . Dotupné také z: http://origin.www.uscc.gov/sites/default/files/Research/China%27s%20Position%20on%20the%20Sony%20Attack_0.pdf

Literatura

ADAMS, James. Virtual Defense: THE WEAKNESS OF A SUPERPOWER. *Foreign Affairs* [online]. 2001, May/June 2001 [cit. 2014-05-18]. Dostupné z: http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

BENCSÁTH, Boldizsár, Gábor PÉK, Levente BUTTYÁN a Márk FÉLEGYHÁZI. 2011. *Duqu: A Stuxnet-like malware found in the wild* [online]. Budapest [cit. 2015-05-06]. Dostupné z: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. Technical Report. Budapest University of Technology and Economics.

FISHMAN, Ted. 2006. *China, Inc.: jak Čína drtí Ameriku a svět*. 1. Praha: Alfa Publishing. ISBN 9788086851440.

FIŘTOVÁ, Magdaléna a Kryštof KOZÁK. 2013. *Spojené státy v úpadku?: Vybrané problémy veřejné politiky v severoamerickém kontextu*. Praha: Dokořán. ISBN 978-80-7363-545-9.

FOOT, Rosemary a Andrew WALTER. 2011. *China, the United States, and global order*. 1. Cambridge: Cambridge University Press. ISBN 9780521725194.

GREENWALD, Glen. 2014. *No place to hide*. London: Penguin Books. ISBN 9780241146699.

HJORTDAL, Magnus. 2001. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* [online]. 4(2) [cit. 2015-05-13]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

CHOI, SeulAh a Gon NAMKUNG. State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era. *The Korean Journal of International Studies* [online]. 2013, 11(2) [cit. 2015-04-26]. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf

KREJČÍ, Oscar. 2009. *Zahraniční politika USA*. Praha: Professional Publishing. ISBN 978-80-7431-003-4.

KWANG, Ho Chun a . 201n. l. *BRICs Superpower Challenge : Foreign and Security Policy Analysis* [online]. Ashgate Publishing Ltd [cit. 2015-05-05]. ISBN 9781409468707. Dostupné z: http://site.ebrary.com/lib/natl/detail.action?docID=10791920

LEWIS, J M. 2010. *Cyberwarfare and its impact on international security*. New York: United Naions Office for Disarmament Affairs, United Nations.

LIEBERTHAL, Kenneth Lieberthal a Wang JISI. THE JOHN L. THORNTON CHINA CENTER AT BROOKINGS. *Addressing U.S.-China Strategic Distrust* [online]. 2012 [cit. 2014-05-18]. Dostupné z: http://www.brookings.edu/~/media/research/files/papers/2012/3/30%20us%20china%20lieberthal/0330_china_lieberthal.pdf

LIEBERTHAL, Kenneth a Peter W. SINGER. The 21st Century Defense Initiative, China Center. *Cybersecurity and U.S.-China Relations* [online]. 2012 [cit. 2014-05-18]. Dostupné

z:http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

LINDSAY, Jon. 2012. *China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops held at the University of California, San Diego* [online]. [cit. 2015-05-13].

LINDSAY, Jon R. 2014. On Cybersecurity The Impact of China on Cybersecurity. *Internal Security* [online]. 39(3) [cit. 2015-05-05]. Dostupné z: http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00189#.VUjmLvntmko

LUM, Thomas, Christopher M. BLANCHARD, Nicolas COOK a Kerry DUMBAUGH. 2010. *China in the 21st Century : China and the U.S. : Comparing Global Influence* [online]. [cit. 2015-05-05]. ISBN 9781616689841. Dostupné z: http://site.ebrary.com/lib/natl/reader.action?docID=10674905

MAZANEC, Brian. 2009. The Art of (Cyber) War. *Journal of International Security Affairs* [online]. (16) [cit. 2015-05-13]. Dostupné z: http://www.securityaffairs.org/issues/2009/16/mazanec.php.

MOHAN, C. Raja. 2013. US-China cyber talks : internet security in the global economy. *RSIS Commentaries* [online].046(13) [cit. 2015-05-13]. Dostupné z: http://dr.ntu.edu.sg/handle/10220/13340

MORRISON, Wayne M. 2015. China-U.S. Trade Issues. *Congressional Research Service* [online]. [cit. 2015-05-09]. Dostupné z: https://fas.org/sgp/crs/row/RL33536.pdf

PARKS, Raymond C. Parks and David P. Duggan. Principles of Cyber-warfare. West Point: United States Military Academy [online]. 2001 [cit. 2015-04-25]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf

PERRY, William G. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *The Center for Security Policy* [online]. 202(28) [cit. 2015-05-05]. Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2007-10-China%20Paper%20Final%20Draft%20%282%29.pdf

SEGAL, Adam M. 2014. Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis* [online]. 38(4) [cit. 2015-05-05]. Dostupné z: http://www.tandfonline.com/doi/pdf/10.1080/09700161.2014.918447#.VUjrufntmko

SCHREIER, Fred. 2012. *On Cyberwarfare: DCAF Horizon 2015 Working Paper Series (7)* [online]. [cit. 2015-05-13]. Dostupné také z: http://www.dcaf.ch/Publications/On-Cyberwarfare

SIDLEY. *New U.S. Sanctions Program Targets Malicious Foreign-Origin Cyber Activities: Sanctions Update*. 2015. Dostupné z: http://www.sidley.com/~/media/update%20pdfs/20150402%20sanctions%20update.pdf

SPADE, Jayson M. 2012. *INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*. Pennsylvania: U.S. ARMY WAR COLLEGE. Dostupné také z: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

ŠTEFANCOVÁ, Vladimíra a René PAWERA. 2013. ČÍNA A SÚČASNÝ MANAŽMENT MEDZINÁRODNEJ BEZPEČNOSTI. Bratislava: *Academia.edu* [online]. [cit. 2015-05-05]. Dostupné z:http://www.academia.edu/6616164/%C4%8C%C3%8DNA_A_S%C3%9A%C4%8CASN%C3%9D_MANA%C5%BDMENT_MEDZIN%C3%81RODNEJ_BEZPE%C4%8CNOSTI

STEVENS, Tim. Apocalyptic Visions: Cyber War and the Politics of Time. *Social Science Research Network* [online]. 2013, 28 [cit. 2015-04-25]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2256370

SWAINE, Michael D. 2013. Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://carnegieendowment.org/files/CLM42MS.pdf

TURNER, Oliver. 2014. *American images of China: identity, power, policy*. 1. London: Routledge. ISBN 9780415659550.

WOMACK, Brantly. 2010. *China among unequals: asymmetric foreign relationships in Asia*. 1. Singapore: World Scientific. ISBN 978-9814295277.

Ostatné

APEC 2014: All Quiet on the Cyber Front? 2014. GADY, Franz-Stefan. *China - US Focus* [online]. [cit. 2015-05-09]. Dostupné z: http://www.chinausfocus.com/peace-security/apec-2014-all-quiet-on-the-cyber-front/

BEINA, Xu. 2014. Media Censorship in China. *Council on Foreign Relations* [online]. [cit. 2015-05-11]. Dostupné z: http://www.cfr.org/china/media-censorship-china/p11515

Aféra Snowden: Ako zmenila Európu? 2014. *EurActiv 2014*[online]. [cit. 2014-09-05]. Dostupné z: http://www.euractiv.sk/parlamentny-spravodaj-000461/zoznam_liniek/afera-snowden-ako-zmenila-europu-000332

Aféra Snowden.2014. *Europska Unia* [online]. [cit. 2014-09-05]. Dostupné z: http://www.europskaunia.sk/afera-snowden

GADY, Franz Stefan. He Axiom Report: Cybersecurity and Its Impact on China-US Relations. In: *East West Institute*[online]. 2014 [cit. 2015-04-25]. Dostupné z: http://www.ewi.info/idea/axiom-report-cybersecurity-and-its-impact-china-us-relations

JONG - CHEN, Jing De. 2014. U.S.-CHINA CYBERSECURITY RELATIONS: UNDERSTANDING CHINA'S CURRENT ENVIRONMENT.*Georgetown Journal of International Affairs* [online]. [cit. 2015-05-05]. Dostupné z: http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/

NAKASHIMA, Ellen. 2013. US Target of Massive Cyber- Espionage Campaign. *Washington Post* [online]. (42) [cit. 2015-05-05]. Dostupné z: http://www.ctcitraining.org/docs/US_Target_of_Massive_Cyber_Espionage_Campaign.pdf
NATO Review. 2011, *Nové hrozby- kybernetické dimenzie* [online]. [cit. 2014-09-23]. Dostupné z: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SK/index.htm

Rosenbach M 2014*, Überwachung all over? - Von NSA zum BND und zurück, lecture notes distributed in Digitalle Schwelle at The University of Technology, Dresden on 3.7.2014.*

SEKERA, Tomáš. 2008. *Kybernetické útoky: Rusko? - Gruzie a svět*. Dostupné také z: http://www.mvcr.cz/soubor/zpravodajstvi-dokumenty-prezentace-spolecnosti-logica.aspx

SOOD, Aditya K. a Richard ENBODY. 2014. U.S. MILITARY DEFENSE SYSTEMS: THE ANATOMY OF CYBER ESPIONAGE BY CHINESE HACKERS. *Georgetown journal of International Affairs* [online]. [cit. 2015-05-05]. Dostupné z: http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/

Transatlantic Trade and Investment Partnership. *Office of the United States Trade Representative* [online]. [cit. 2015-05-10]. Dostupné z: https://ustr.gov/ttip

Trans-Pacific Partnership Agreement. *Electronic Frontier Foundation: Defending your rights in the digital world* [online]. [cit. 2015-05-10]. Dostupné z: https://www.eff.org/issues/tpp

U.S. targets overseas cyber attackers with sanctions program. In: MASON, Jeff a Andrea SHALAL. *Reuters.com* [online]. 2015 [cit. 2015-04-26]. Dostupné z: http://www.reuters.com/article/2015/04/01/us-usa-cybersecurity-idUSKBN0MS4DZ20150401

White House Profile: Michael Daniel Special Assistant to the President and Cybersecurity Coordinator. *The White House Blog* [online]. [cit. 2015-05-09]. Dostupné z: https://www.whitehouse.gov/blog/author/Michael%20Daniel

4 ways US can boost cyber security. In: *The Christian Science Monitor* [online]. n.d. [cit. 2015-04-25]. Dostupné z:http://www.csmonitor.com/Commentary/Opinion/2013/0409/4-ways-US-can-boost-cyber-security/Start-where-countries-agree

Tabuľky, obrázky

CHOI, SeulAh a Gon NAMKUNG. *State-led Back-scratching Alliance: The Chinese Government as the Umbrella* [obrázok]. In: State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era [online]. CHOI, SeulAh a Gon NAMKUNG, 2013, [vid. 2015-05-10]. č.2. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf

CHOI, SeulAh a Gon NAMKUNG. *The Cases of China's Cyber Warfare against the United States* [tabuľka]. In: State-led Back-scratching Alliance in Cyber Warfare: China's Strategies in Sino-American Cyber Warfare in the Post-Cold War Era [online]. CHOI, SeulAh a Gon NAMKUNG,

2013, [vid. 2015-05-10]. č.2. Dostupné z: http://www.kaisnet.or.kr/resource/down/11_2_03.pdf; upravené

MAZANEC, Brian M. *Summary of nation – state cyberwarfare capabilities* [tabuľka]. In: *THE ART OF (CYBER) WAR* [online]. MAZANEC, Brian M, 2009, [vid. 2015-05-10]. č.2. Dostupné z: http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf

Univerzita Karlova v Praze
Fakulta sociálních věd
Institut politologických studií

Projekt diplomové práce

Kybernetická bezpečnost: vztah USA a Číny

Autor práce**: Bc.Barbora Debnárová**
Vedoucí práce**: PhDr. Vít Střítecký, M.Phil., Ph.D.**

Téma práce:

Obidve krajiny, USA i Čína, zastávajú význačné role v oblasti svetovej politiky. Dokonca je možné zhodnotiť, že ich vzájomný vzťah je najdôležitejším vzťahom medzi štátmi- v súčasnosti a aj do budúcnosti. Oba totiž majú veľmi významné postavenie v mnohých kritických globálnych záležitostiach, ako je mier a bezpečnosť, obchod, financie či životné prostredie. Z uvedeného teda vyplýva, že to, ako s týmto vzťahom naložia, neovplyvní len ich vlastnú budúcnosť, ale aj budúcnosť celého sveta.

Tento vzťah je už však od vytvorenia Čínskej ľudovej republiky v roku 1949 komplikovaný a poznačený vzájomnou nedôverou. V rámci všetkých problematických záležitostí, kybernetická bezpečnosť je tou, ktorá vytvorila najväčší rozruch v najkratšom čase. Tento krátky časový interval sa dá jednoducho vysvetliť technickým rozvojom a enormným nárastom v používaní informačných technológií za posledné roky.[187]

Dôležitým faktom však ostáva ohromná závislosť USA na informačných technológiách. Spojené štáty sa po studenej vojne stali neporaziteľnou mocnosťou v oblasti konvenčnej aj jadrovej sily. Avšak, ich vojenská neporaziteľnosť a vedúca pozícia v oblasti informačných technológií z nich takisto urobila krajinu najzraniteľnejšiu kybernetickým útokom. Nepriateľ je si v tomto prípade vedomý, že vo vojenskej oblasti nedokáže uspieť, a tak hľadá alternatívne metódy útoku. Kybernetický priestor sa v dnešnej dobe stal priestorom ideálnym pre tieto typy útokov. Závislosť USA na informačných technológiách sa teda môže stať Achillovou pätou tohto zdanlivo neohroziteľného štátu.[188]

Čínska ľudové republika naopak zastáva prominentnú pozíciu medzi krajinami prevádzajúcimi kybernetické útoky na iné štáty. Jej hlavným cieľom je Taiwan, no často sú napádané aj inštitúcie iných zemí, predovšetkým noviny, ministerstvá, ambasády, vládne a nevládne organizácie. Faktom je, že Číňania už od roku 1991 vyvíjajú a dosadzujú pokročilé technológie do ich vlády, vojenského a civilného sektoru v rámci úsilia o vybudovanie čínskej hospodárskej a politickej sily. Okrem toho je toto považované za úsilie o vytvorenie protiváhy k americkej vojenskej nadradenosti. Ba čo viac, Čína uznáva kybernetický priestor ako

[187] M. SPADE, Jayson. U.S. ARMY WAR COLLEGE. *INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY* [online]. 2012 [cit. 2014-05-18]. Dostupné z:http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

[188] Ibid

bojovú doménu a kybernetickú moc dáva do jednej roviny s pozemskou, vodnou a vzdušnou vojenskou silou.[189]

Zdôvodnenie voľby témy:

Danú tému som si vybrala predovšetkým preto, lebo je prienikom bezpečnosti a informatiky, teda dvoch odborov, ktoré študujem. Problematika kybernetickej bezpečnosti je navyše veľmi aktuálna s potenciálom do budúcnosti. Čína a USA sa dajú považovať sa dvoch najdôležitejších aktérov na tomto poli. Na túto tému už vznikla nejaká literatúra, no z dôvodu jej relatívnej novosti predpokladám, že táto problematika nie je ešte celkom preskúmaná a myslím, že sa v tejto oblasti stále dá priniesť niečo nové.

Cieľ práce a výskumná otázka:

Cieľom mojej diplomovej práce je previesť analýzu vzťahu USA a Číny so zameraním na kybernetickú bezpečnosť a na základe tejto analýzy zodpovedať na výskumnú otázku, ktorá znie: ako problematika kybernetickej bezpečnosti ovplyvňuje vzájomné vzťahy Číny a USA?

Hypotéza:

Hypotézou je, že problematika kybernetickej bezpečnosti výrazne vplýva na politické, obchodné, investičné, vojenské a ďalšie aspekty vzťahu Číny a USA. Zvyšuje dynamiku vzájomných jednaní, napätie medzi štátmi a obe krajiny núti prijímať rôzne opatrenia v priamej či nepriamej súvislosti s kybernetickou bezpečnosťou a tým druhým štátom.

Teoretické ukotvenie:

Ako teoretické východisko vo svojej práci použijem realistický pohľad na kybernetickú bezpečnosť, konkrétne myšlienky vyslovené neorealistickým autorom Jamesom Adamsom. Adams je zakladateľom a predsedom iDefense, firmy zaoberajúcej sa kybernetickou inteligenciou a riadením rizika a členom the National Security Agency Advisory Board. James Adams hľadí na internet ako na anarchický systém, v ktorom absentuje nejaká riadiaca organizácia a polícia. Vyhlasuje, že kyber priestor sa stal novým svetovým bojiskom. Každý štát v ňom stojí sám alebo so spojencami, ktorým nikdy nemôže dôverovať. V zúfalstve sa

[189] Ibid

snaží získať kybernetickú obranu a silu, pretože má strach, že každý krok iného štátu môže symbolizovať priamu hrozbu pre jeho vlastnú bezpečnosť.[190]

Na margo národnej bezpečnosti Spojených štátov v spojitosti s kybernetickou bezpečnosťou Adams tvrdí, že z nich ich vojenská a technologická nadradenosť urobila kybernetickými útokmi najzraniteľnejšiu krajinu.[191]

Čínu označuje za najnebezpečnejšiu krajinu v kyber priestore. [192]

Metodológia a operacionalizácia:

Ako výskumnú metódu som zvolila jedno- prípadovú štúdiu. Konceptom je pojem kybernetickej bezpečnosti. Závislou premenou bude vzťah Číny a USA a jeho rôzne dimenzie. Nezávislými premennými budú napríklad dialóg USA a Číny o kybernetickej bezpečnosti a opatrenia prijaté v tejto oblasti. Operacionalizácia konceptu vyžaduje jeho premenu na indikátory. Indikátormi v tomto prípade budú rôzne typy kybernetických útokov, predovšetkým špionáž, známe aféry v oblasti kybernetickej bezpečnosti (Snowden a pod.), inteligenčné operácie atď.

Kritika zdrojov:

Ako zdroje budú použité hlavne monografie vydané kompetentnými organizáciami, knihy zaoberajúce sa kybernetickou bezpečnosťou či články z vedeckých časopisov. Teoretické východisko zakladám na článku Jamesa Adamsa s názvom *„Virtual Defense“*. Ako odrazový zdroj bude použitá správa organizácie MANDIANT- *„APT1: Exposing One of China's Cyber Espionage Units“.* Za užitočný dokument tiež považujem *„Cybersecurity and U.S.-China Relations“* vydaný *The 21st Century Defense Initiative* v spolupráci s *China Center,* v ktorom je preukázaná snaha pochopiť kľúčové trendy a riziká v kybernetickom priestore a na základe týchto poznatkov pochopiť vzájomné vzťahy Číny a USA v tejto problematike. Ďalším významným zdrojom bude dokument „*INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY*“ vydaný *U.S. ARMY WAR COLLEGE* zaoberajúci sa čínskou hrozbou pre americkú národnú bezpečnosť. Ďalším zo zdrojov významných pre túto prácu bude kniha od Václava Jirovského „*Kybernetická kriminalita:*

[190] ADAMS, James. Virtual Defense: THE WEAKNESS OF A SUPERPOWER. *Foreign Affairs* [online]. 2001, May/June 2001 [cit. 2014-05-18]. Dostupné z: http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

[191] Ibid
[192] Ibid

nejen o hackingu, crackingu, virech a trojských koních bez tajemství" vysvetľujúca technické záležitosti z oblasti kybernetickej kriminality.

Predpokladaná štruktúra práce:

1. Úvod

1.1.Ciele práce

1.2.Obsah

1.3.Metodológia a použitá teória

2. Vzťahy Číny a USA všeobecne : od 49 po súčasnosť

2.1. História

2.2.Súčasnosť

2.1.1. Vplyv histórie na súčasnosť

2.1.2. Ekonomické, politické a iné typy medzinárodných vzťahov

2.1.4. Ako USA vníma Čínu

2.1.5. Ako Čína vníma USA

3. Kyber priestor a kybernetická bezpečnosť

3.1. Dôležité pojmy a súvislosti

4. Čína v kyber priestore

4.1.National Cybersecurity Policy

4.2.Information Warfare Doctrine

4.3.Intelligence Issues: Chinese Intelligence Operations and Transnational Consequences

4.4.Military Organizations

4.5.Economic Drivers

4.6.Rastúci kybernetický zločin

4.7.Comparative Perspectives

5. Vplyv problematiky kybernetickej bezpečnosti na vzájomné vzťahy USA a Číny

5.1.Kybernetická bezpečnosť a nedôvera v americko- čínskych vzťahoch

5.1.1. Čínska špionáž

5.1.2. Snowden a iné aféry

5.2.Kybernetická bezpečnosť ako politický problém

Predpokladaná literatúra:

obecné zdroje –

DUNNIGAN, James F. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*. Vyd. 1. Praha: Baronet, 2004. 356 s. ISBN 80-7214-642-4.

EICHLER, Jan. *MEZINÁRODNÍ BEZPEČNOST NA POČÁTKU 21. STOLETÍ*. Praha: Ministerstvo obrany České republiky – AVIS, 2006. ISBN 80-7278-326-2.

JIROVSKÝ, Václav. *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.

monografie-

China and Cybersecurity: Political, Economic, and Strategic Dimensions [online]. San Diego, 2012 [cit. 2014-05-18]. Dostupné z: http://igcc.ucsd.edu/assets/001/503568.pdf. Report from Workshops held at the University of California, San Diego. University of California, Institute on Global Conflict and Cooperation.

Cybersecurity for State Regulators: With Sample Questions for Regulators to Ask Utilities [online]. 2013 [cit. 2014-05-18]. Dostupné z: http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf. Report. The National Association of Regulatory Utility Commissioners.

IOSCO RESEARCH DEPARTMENT AND WORLD FEDERATION OF EXCHANGES. Cyber-crime, securities markets and systemic risk. In: [online]. 2013 [cit. 2014-02-13]. Dostupné z: http://www.world-exchanges.org/files/statistics/pdf/IOSCO_WFE_Cyber-crime%20report_Final_16July.pdf

LEWIS, J. UNODA. *Cyberwarfare and its impact on international security*. New York, 2010.

LIEBERTHAL, Kenneth a Peter W. SINGER. The 21st Century Defense Initiative, China Center. *Cybersecurity and U.S.-China Relations* [online]. 2012 [cit. 2014-05-18]. Dostupné z:http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

MANDIANT. *APT1: Exposing One of China's Cyber Espionage Units*. 2013, 76 s. Dostupné z: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

M. SPADE, Colonel Jayson. U.S. ARMY WAR COLLEGE. *INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY* [online]. 2012 [cit. 2014-05-18]. Dostupné z:http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf

POŽÁR,, Josef. *Některé aspekty kybernetické kriminality* [online]. Praha, 2011 [cit. 2014-02-13]. Dostupné z: http://www.cybersecurity.cz/data/Pozar.pdf. Prezentace. Policejní akademie České republiky v Praze.

články vo vedeckých časopisoch-

ADAMS, James. Virtual Defense: THE WEAKNESS OF A SUPERPOWER. *Foreign Affairs* [online]. 2001, May/June 2001 [cit. 2014-05-18]. Dostupné z: http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

CHEN, Jeffrey. Snowden, Cybersecurity, and China-US Relations. *Fair Observer* [online]. 2013 [cit. 2014-05-18]. Dostupné z: http://www.fairobserver.com/region/north_america/snowden-cybersecurity-and-china-us-relations/

Cyber Security and the Intelligence Community. In: *Belfer Center: for Science and International Affairs* [online]. 2009 [cit. 2014-05-11]. Available from:http://belfercenter.ksg.harvard.edu/publication/19158/cyber_security_and_the_intelligence_community.html

FARNSWORTH, Timothy. U.S., China Meet on Cybersecurity. *Arms Control Association* [online]. 2013 [cit. 2014-05-18]. Dostupné z: http://www.armscontrol.org/act/2013_09/US-China-Meet-on-Cybersecurity

pramene a ostatné zdroje-

Kybernetická kriminalita IV: Hacktivismus a kyberterorismus. In: *BusinessIT* [online]. 2012 [cit. 2014-02-13]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

J. PETALLIDES, Constantine. Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New. *Student Pulse* [online]. 2012, 2012, VOL. 4 NO. 03 | PG. 1/1 [cit. 2014-05-18]. Dostupné z:http://www.studentpulse.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat

NSA spying scandal: Barack Obama signals review of surveillance programmes following Edward Snowden revelations. In:*The Independent* [online]. 2013 [cit. 2014-05-11]. Available from: http://www.independent.co.uk/news/world/americas/nsa-spying-scandal-barack-obama-signals-review-of-surveillance-programmes-following-edward-snowden-revelations-9019547.html