Anotace: Tento příspěvek, „poskládaný“ výhradně z informací, dostupných v rámci otevřených zdrojů, se pokouší alespoň indikativně nastínit situaci v některých zemích světa, které je možné označit za „důvodně podezřelé“ z řady defensivních a ofensivních aktivit v oblasti kyberprostoru. Pozornost je věnována institucionálnímu podchycení této agendy (konkrétní agentury a náplň jejich činnosti) a podle možností i některým dalším aspektům sledovaného tématu.

Klíčová slova: kybernetická válka, kyberzbraně, kyberútok, bezpečnostní komunita

RNDr. Václav Hník, CSc., Mgr. Oldřich Krulík, Ph.D., doc. RNDr. Josef Požár, CSc.[1]

Kybernetická válka optikou některých „pokročilých států světa

Tento příspěvek, „poskládaný“ výhradně z informací, dostupných v rámci otevřených zdrojů, se pokouší alespoň indikativně nastínit situaci v některých zemích světa, které je možné označit za „důvodně podezřelé“ z řady defensivních a ofensivních aktivit v oblasti kyberprostoru. Ačkoli se zdaleka nejedná o dokonalé vyčerpání tohoto tématu, mohou být některá jeho zjištění pro širší odbornou veřejnost zajímavá.

Spojené státy americké

Kybernetické bezpečnosti (a pochopitelně i jejímu aktivnímu prosazování) se v rámci Spojených států amerických věnuje několik vládních agentur.

První, o kterém bude řeč, je **Kybernetické velitelství** (*United States Cyber Command, USCYBERCOM, CYBERCOM*).[2]

CYBERCOM funguje od roku 2009 a plné funkcionality dosáhl v květnu 2010. Začleněn je v rámci Strategického velení Ministerstva obrany USA. Jeho součásti jsou složky z pozemních, námořních i leteckých sil. Jeho úkolem je plánovat, koordinovat, integrovat, synchronizovat a provádět veškeré vojenské operace v kyberprostoru, zajistit v něm svobodu jednání USA i jeho spojencům a „zabránit tomu samému (tedy za učitých okolností pro USA nežádoucímu svobodnému jednání) našim nepřátelům„ („*deny the same to our adversaries*“).

Generál Keith Alexander v této souvislosti při slyšení před Kongresem explicitně prohlásil, že Spojené státy v kyberprostoru podle potřeby aktivně útočí bez ohledu na to, je-li jim identita útočníka známa, či nikoli.

Dalším subjektem hodným pozornsoti je **Centrum kybernetické kriminality** při Ministerstva obrany (*Department of Defence Cyber Crime Center, DoD CCC, DC3*) [3]

D3C je složkou, která vyvíjí specializovanou činnost v oblasti kybernetické bezpečnosti. Jeho činnost je zaměřena především na analýzu digitálních stop na veškerých digitálních mediích a stanovení standardů forenzních digitálních důkazů. V případě potřeby spolupracuje při vyšetřování vojenských trestných činů povahy kriminální, zpravodajské i teroristické. Kromě vlastního forenzního zkoumání, školí forenzní specialisty a provádí vlastní výzkum.

[1] Pracovníci Policejní akademie České republiky v Praze. Kontakt: hnik@polac.cz, krulik@polac.cz, pozar@polac.cz.
[2] United States Cyber Command: Cyber Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.defense.gov/home/features/2010/0410_cybersec/>.
[3] Department of Defense Cyber Crime Center (DC3) [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dc3.mil/home.php>.

Národní bezpečnostní agentura (*National Security Agency / Central Security Service – NSA/CSS*)[4] spadá rovněž pod Ministerstvo obrany. Platformy

NSA a *CSS* vznikly každá v různou dobu a jejich úkoly jsou poněkud odlišné. V současnosti však bylo jejich velení spojeno a navenek se jeví spíše jako organizace jediná. Tato organizace vyvíjí specializovanou činnost v oblasti kryptologické, a to jak v oblasti rozvědné zpravodajské činnosti (sběr i ananlýza zpráv zahraničních rozvědek) i činnosti kotrarozvědné (ochrana vládních informačních sítí). Provádí odposlechy telefonních hovorů, radiového komunikace, e-mailů i dalšího internetového provozu. *NSA* hraje velmi důležitou roli v ochraně federálních počítačových sítí proti kyberterorismu[5] Jako zvláštnosti je možné uvést, že pomocí speciálních systémů na dně oceánů údajně podává vládě USA zprávy o pohybu lodí i ponorek. Analýza a vytváření kryptované komunikace je finančně, technicky i lidsky velmi náročná. Již v roce 2002 byla *NSA* pravděpodbně největším zaměstnavatelem matematiků v USA[6], rozhodně není překvapivé, když se v minulosti objevila zpráva[7], že *NSA* vlastní největší skupinu suprepočítačů ve Spojených státech.

Výše uvedené instituce, zvláště *CYBERCOM* a *NSA*, „vedou válku" v doméně .mil. V druhé hlavní vládní doméně USA, doméně .gov. „bojuje" **Ministerstvo vnitřní bezpečnosti** (*Departement of Homeland Security, DHS*). Ministerstvo vznikla v roce 2003. Jedná se o strukturu s téměř čtvrt milónem zaměstnanců, která pokrývá mnoho bezpečnostních oblastí. Kybernetické bezpečnosti se věnuje zejména jeho **Kancelář pro kybernetickou bezpečnost a komunikace** (*Office of Cybersecurity and Communications, CS&C*), která byla vytvořena v roce 2006. *CS&C* je zodpovědná za zajištění bezpečnosti, odolnosti a spolehlivosti národní kybernetické a komunikační infrastruktury.[8]

Tato aktivita zahrnuje nejen oblast vládních (veřejných) infrasturktur, ale i infrastruktury privátní. Katastrofickým incidentům, které by tuto infrastrukturu mohly narušit nebo zničit se snaží aktivně předcházet, přípravit se na ně a reagovat na ně. Jako agentura odpovědná za bezpečnost v určité oblasti koordinuje národní reakci na krize v rámci tzv. „**Národního rámce odpovědnosti**" (*National Response Framework, NRF*)[9] a řídí další specializované agentury v rámci Ministerstva, zejména již dříve (v roce 2003) vytvořenou **Národní sekci pro kybernetickou bezpečnost** (*National Cyber Security Division, NCSD*).[10]

[4] National Security Agency [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.nsa.gov/>.
[5] NAKASHIMA, Ellen, Bush Order Expands Network Monitoring; in: The Washington Post, 26. I. 2008 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html>.
[6] Statement for the Record before the Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services Hearing on Critical Skills for National Security and the Homeland Security Federal Workforce Act. National Security Agency, 12. III. 2002 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.nsa.gov/public_info/speeches_testimonies/12mar02.shtml>.
[7] SHANE, Scott; BOWMAN, Thomas, No Such Agency; in: Baltimore Sun, 4. XII. 1995. [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://cryptome.org/jya/nsa-sun.htm>.
[8] Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/index.shtm>.
Protect Myself Online; in: Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/files/cybersecurity.shtm>.
KRULÍK, Oldřich. Místo a úkoly Ministerstva vnitřní bezpečnosti USA; in: Obrana a strategie. 2003, č. 2, s. 139 až 162. ISSN 1214-6463. Poznámka: Článek byl redakcí pro potřeby anglickojazyčné mutace časopisu přeložen a paralelně vydán pod názvem „Role and Mission of the U. S. Department of Homeland Security".
[9] National Response Framework Resource Center; in: FEMA [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.fema.gov/emergency/nrf/>.
[10] Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/index.shtm>.

Zdá se[11], že v minulosti doprovázely *NCDS* určité organizační a personální problémy (projevující se navenek častým střídáním vedení), v současnosti je pravděpodobně situace již stabilizovaná. *NCDS* na svých stránkách[12] deklaruje, že dosahuje svých strategických cílů prostředníctvím následujících programů:

- Národní systém reakce v kyberprostoru (*National Cyberspace Response System*), který si klade za úkol zajišťovat nepřetržitou ochranu kybernetické informační infrastruktury. To zahrnuje zejména:
    - přípravu v oblasti kybernetické bezpečosti a **Národní systém kybernetické výstrahy** (*National Cyber Alert System*);[13]
    - centrální organizaci typu **CERT** (*United States Computer Readiness Team, US-CERT*);[14]
    - **Národní skupinu pero koordinaci kybernetické reakce** (*National Cyber Response Coordination Group*) vytvořenou ze 13 federálních agentur;
    - *Cyber Cop Portal* s úkolem sdílet a koordinovat informace směřující k zadržení a usvědčení pachatelů kybernetických zkočinů.

- Systém jednotlivých kontaktních bodů pro bezpečnost federální kybernetické infrastruktury (*Federal Network Security*)[15].

- Program řízení kybernetického rizika, zahrnující zejména
    - mezinárodní[16] cvičení v oblasti kybernetické bezpečnosti **Cyber Storm**;[17]
    - pravidelný „Měsíc národní osvěty v oblasti kybernetické bezpečnosti“ (*National Cybersecurity Awareness Month*)[18], pořádaný každý říjen a program zajištění bezpečnosti počítačového softwaru.

[11] Wikipedia: National Cyber Security Division [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://en.wikipedia.org/wiki/national_cyber_security_division>.
[12] National Cyber Security Division; in: Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/xabout/structure/editorial_0839.shtm>.
[13] Mailing Lists and Feeds; in: US-CERT, Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.us-cert.gov/referral_pg/>.
[14] Current Activity; in: US-CERT, Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.uscert.gov/>.
[15] About Federal Network Security; in: Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/xabout/structure/gc_1279034068412.shtm>.
[16] Posledního mezinárodního cvičení Cyber Strom III v září 2010 se kromě USA zúčastnilo již 12 daších zemí včetně Maďarska jako první postkomunistické země. Česká republika mezi nimi nebyla.
Cyber Storm III [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf>.
[17] Cyber Storm: Securing Cyberspace; in: Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/files/training/gc_1204738275985.shtm>.
[18] National Cyber Security Awareness Month; in: Homeland Security [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.dhs.gov/files/programs/gc_1158611596104.shtm>.

Ruská federace

Podle „většinového“ názoru[19] jsou organizace, které v rámci Ruské federace vyvíjejí aktivity související s informační válkou, následující:[20]

Federální ochranná služba (*Федеральная служба охраны*, *Federaľnaja služba ochrany – ФСО*, *FSO*)[21]

Platforma zajišťuje fyzickou ochranu včetně ochrany soukromí a komunikací nejvyšším státním činitelům a zvláště prezidentovi. Patří do ní i ostraha Kremlu. Podle odhadů zaměstnává přibližně 20 000 – 30 000 lidí. Převzala řadu služeb od zrušené *FAPSI*. Jejími úkoly je mimo jiné poskytování zpravodajských informací, odposlech telefonní, bezdrátové, internetové i satelitní komunikace a provozování důležitých vládních komunikací.

Federální bezpečnostní služba (*Федеральная служба безопасности Российской Федерации – ФСБ*, *FSB*)[22]

Služba zdědila největší podíl od svého předchůdce – *KGB*, včetně sídla v Ljublance[23]. Počet jejich zaměstnanců je odhadován na 200 000 – 300 000 osob, větší část z nich nicméně patrně nevykonává zpravodajskou činnost, ale pracuje v oblasti ochrany státních hranic, boji proti organizovanému zločinu, drogám a terorismu.

FSB působí v doma i v zahraničí (ve spolupráci se *SVR*, viz níže). Vyvíjí široké spektrum zpravodajských činností, ale i takové záležitosti jako bezpečnostní pověrky a boj proti organizovanému zločinu. Realizuje odposlechovou činnost telefonní i internetové komunikace, kontroluje poštovní zásilky. Pokud se jedná o internet, provozuje FSB pravděpodobně systém *SORM II*, jakousi analogii systému *Carnivore*, který provozuje *FBI* a který údajně umožňuje monitorovat veškerý internetový provoz v rámci Ruské federace. Není příliš překvapivé, že služby jako Skype, Gmail a Hotmail se takovým aktivitám brání a že se čas od času vynoří informace o činnosti *FSB* v této souvislosti. *FSB* od *FAPSI* zdědila systém operačních center, umožňujících kryptologické analýzy. Služba pravděpodobně disponuje schopností sofistikovaných kybernetických „aktivních opatření”.

---

[19] HEICKERÖ, R. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www2.foi.se/rapp/foir2970.pdf>.
Soviet/Russian Intelligence Agencies; in: FAS Intelligence Resource Program [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.fas.org/irp/world/russia/index.html>.
Soviet/Russian Intelligence Agencies; in: Intelligence Resources Program [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.agentura.ru/english/equipment/>.
LEYDEN, J., Russian Spy Agencies Linked to Georgian Cyber-Attacks; in: The Register, 23. III. 2009 [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/>.
Cyber Warfare: Project Grey Goose Phase II Report on India; in: Intelli Briefs [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://intellibriefs.blogspot.com/2009/03/cyber-warfare-project-grey-goose-phase.html>.
Geopolitic Cyber Sources; in: Emil on Security, 10. IX. 2010 [online; citováno 6. IX. 2011]. Dostupné z WWW: <https://emilonsecurity.wordpress.com/2010/09/10/geopolitic-cyber-forces/>.

[20] K těmto platformám je třeba ještě připočítat dnes již samostatně neexistující *FAPSI*, viz níže.

[21] ФСО [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.fso.gov.ru/>.

[22] Federaľnaja služba bezopasnosti [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.fsb.ru>.

[23] Funding for the Russian Secret Services; in: Agentura.ru [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.agentura.ru/english/experts/safranchuk/>.

Služba zahraniční rozvědky (*Служба Внешней Разведки***, *Služba vnešnej razvedky* – *СВР*, *SVR*)**[24]

Zpravodajská služba zaměřená na působení v zahraničí. Odhady počtu zaměstnanců uvádějí číslo 15 000[25]. Zde vyvíjí široké spektrum „aktivních opatření" včetně elektronického odposlechu. Když tehdejší prezident Putin uváděl v roce 2007 do funkce současného ředitele *SVR* Michaila Fradkova prohlásil,[26] že mezi hlavní priority zahraniční rozvědky *SVR* patří boj proti mezinárodnímu terorismu a pomoc při „posilování ruského průmyslového a obranného potenciálu" (což je mimo jiné eufemismus pro oblast průmyslové špionáže).

Hlavní zpravodajská správa (*Главное Разведывательное Управление*, *Glavnoe razvědyvatělnoje upravlenie* – *ГРУ*, *GRU*)

GRU je vojenská zpravodajská služba. Odhady hovoří o několikanásobně větším počtu zaměstnanců než počet zaměstnanců „civilní" rozvědky *SVR*. Byla založena v roce 1918 a na rozdíl od *KGB* přečkala různé reorganizace po rozpadu Sovětského svazu. Je proto možné konstatovat, že od roku 1918 existovala kontinuálně až do dnešních dnů. Jejím úkolem je získávat všekeré vojensky významné zpravodajské informace zejména ze zahraničí. Služba provozuje radiové zpravodajství (*SIGINT – Signals Intelligence*) prostřednictvím pozemních stanic (na Kubě a v pobaltských státech) i pomocí vlastních satelitů.

Zpracování takto získaných dat je značně nákladné a vyžaduje velký počet[27] velmi kvalifikovaných pracovníků schopných provádět potřebnou analýzu signálů i jejich případné dešifrování. To znamená, že *GRU* má nepochybně i „kvalifikaci" pro kybernetickou válku. Pod vedení *GRU* jsou zařazeny mimo jiné i jednotky speciálních sil Spetznaz, které vykonávají elektronickou zpravodajskou činnost vojenského zaměření.

Federální agentura pro vládní komunikaci a informace (*Федеральное Агентство Правительственной Связи и Информации*, ***Federaľnoje Agenstvo Praviteľstvennoj Svajazi i Informacii*** **–** ФАПСИ, ***FAPSI*****)**[28]

FAPSI (zrušená dekretem z března 2003 a její agenda rozdělena mezi FSB a Ministerstvo obrany) byla elektronická odposlechová služba analogická americké *NSA* nebo britské *GCHQ*. Vznikla počátkem devadesátých let sloučením 8. a 16. hlavní správy někdejší *KGB*, v roce 2003 byla reorganizována a její složky zařazeny pod FSB a některé patrně i pod *GRU*, *SVR* a *FSO*. Oficiálně uváděný důvod bylo obvinění z korupce. Její oficiální a utajovaný název zněl „**Hlavní ředitelství radiolektronické rozvědky v sítích Svazu**" (*Glavnoye Upravlenie Radioelectronnoi Razvedki Na Setyah Svyazi*,

[24] Служба внешней разведки Российской Федерации [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://svr.gov.ru/>.
[25] SVR: Russian Intelligence Service; in: Agentura.ru [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.agentura.ru/english/dosie/brit/svr/>.
[26] PACNER, K., Nová ofenzíva ruských rozvědek, 1. IX. 2008 [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.karelpacner.cz/?str=hom&id=219&n=nova-ofenziva-ruskych-rozvedek>.
[27] Počátkem devadesátých let pracovalo v oblasti SIGINT v Sovětském svazu odhadem celkem (tj. KGB a GRU dohromady) 350 000 osob, přičemž aktivity GRU byly patrně rozsáhlejší.
GLASSER, R., Signals Intelligence and Nuclear Preemption, 1989 [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.carlisle.army.mil/usawc/parameters/articles/1989/1989%20glasser.pdf>.
GRU; in: Global Security [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.globalsecurity.org/intell/world/russia/gru.htm>.
[28] Wikipedia: FAPSI [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://en.wikipedia.org/wiki/fapsi>.
FAPSI (Federaľnoje Agenstvo Praviteľstvennoj Svajazi i Informacii); in: specialista.cz, 31. X. 2005 [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://magazin.specialista.info/rservice.php?akce=tisk&cisloclanku=2005103101%20target=>.

GURRSS). Zajímala se o veškeré informace politického, ekonomického, vojenského a vědeckého charakteru a zřejmě byla schopná odposlouchávat veškerou vládní i soukromou komunikaci v zemi, včetně komunikace po internetu.

FAPSI dostala možnost podnikat, které intenzivně využívala (např. její „bezpečnostní“ programy povinně kupovaly vládní orgány). Provozovala vládní a prezidentský informační systém i internetového providera, jehož služby nabízela vládním složkám. Ostatní provideři museli povinně instalovat program od *FAPSI*, který umožňoval monitorovat jejich provoz. V zemi v té době nebylo možno používat kryptografický program jiného výrobce než *FAPSI*. *FAPSI* vyvíjela činnost i v zahraničí, v některých zemích provozovala i odposlechová centra.[29]

Poznámka: Všechny uvedené organizace (a nejenom ony) vznikly počátkem devadesátých let rozdělením někdejšího **Výboru pro státní bezpečnost** (*Комитет государственной безопасности, КГБ, KGB*). Počty zaměstnanců (a ještě více rozpočty) zpravodajských služeb Ruské federace jsou utajovány.[30] Jaký podíl z celkové činnosti těchto služeb je věnován kybernetické válce se můžeme jen dohadovat. Velmi mimimalistický odhad znamená, že se této činnosti intenzívně věnuje několik tisíc jedinců.

Čínská lidová republika

Dostupné zdroje informací o aktivitách Čínské lidové republiky v oblasti informační války[31] se v zásadě shodují, že země se této záležitosti intenzivně věmuje již od počátku devadesátých let a že je v této oblasti velmi pokročilá.

Tamější vojenští teoretici, plánovači a velení si patrně velmi dobře uvědomují relativní přednosti informační války a její roli v možném budoucím globálním válečném střetnutí. Kybernetická válka je chápána jako důležitá složka třetího (tzv. „bezkontaktního“) pilíře konceptu tzv. „tří válek“ a jako příklad asymetrického a pokud možno lokálního konfliktu se silnou rolí informačních technologií. Některé zdroje[32] tuto zemi ji (spolu s Indií) kladou na vyšší úroveň než Ruskou federaci. Do jaké míry je tomu skutečně tak, je otázka.

Základní předpoklad však Čína nepochybně splňuje, a to dostatek finančních prostředků. Příprava a vedení kybernetické války (v míře v globálním měřítku významné) je velmi nákladná záležitost,

[29] Cyber Wars; in: Agentura.ru [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.agentura.ru/english/equipment/>.
[30] Safrančuk; in: Agentura.ru [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.agentura.ru/english/experts/safranchuk/>.
Center for Defense Information [online; citováno 6. IX. 2011]. Dostupné z WWW: <http://www.cdi.org/>.
[31] De WEESE, Steve; KREKEL, Bryan a kolektiv, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation, 9. X. 2009 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.uscc.gov/researchpapers/2009/northropgrumman_prc_cyber_paper_final_approved%20report_16oct2009.pdf >.
VENTRE, Daniel, Chinese Information and Cyber Warfare; in: e-International Relations, 13. IV. 2010 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.e-ir.info/?p=3845>.
LIANG, Qiao; XIANGSUI, Wang, Unrestricted Warfare, PLA Literature and Arts Publishing House, Beiing, February 1999 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://cryptome.org/cuw.htm>.
[32] MAZANEC, Brian, M., The Art of (Cyber) War; in: The Journal of International Security, Spring 2009, No 16 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.securityaffairs.org/issues/2009/16/mazanec.php>.

a proto si to mohou „dovolit“ jen státy dostatečně bohaté (a ovšem výjimečně a v určité oblasti i státy chudé, pokud to „nemusí nikomu vysvětlovat“, příkladem jsou možné aktivity Severní Koreje v této oblasti), a to Čínská lidová republika v poslední dekádě určitě je. Její obranný rozpočet (oficiálně oznámený i odhadovaný skutečný) v posledních letech podle nejnovější dostupné zprávy amerického ministerstva obrany o vojenských schopnostech Čínské lidové republiky za rok 2008 vytrvale roste průměrně o 10 % ročně.[33] V roce 2007 byl odhadovaný skutečný vojenský rozpočet „říše středu“ 2–3 krát větší než obdobný rozpočet Ruské federace.

Které státní orgány se kybernetické válce věnují, se Peking snaží intentzivně utajovat stejně jako Moskva. Citovaná americká zpráva za rok 2008 v této souvislosti zmiňuje čínskou armádu a „*další prvky vlády ČLR*“ („*other elements of the PRC government*“). Analogické zprávy za rok 2006[34] a 2004[35] v souvislosti s kybernetickou válkou uvádějí vždy jen čínskou armádu („*PLA*“ – viz logo).[36]

Americkým analytikům se však podařilo sestavit o této záležitosti poměrně detailní obraz. V posledních letech však lze identifikovat i známky určitého uvolnění a některé informace začínají být zveřejňovány (například článek[37] o výzkumu dvou scénářů kybernetického útoku na elektrické sítě ve Spojených státech). Také se zdá[38], že tyto aktivity nabývají i jistou civilní dimenzi a že v Čínské lidové republice v oblasti informační války dochází i k nějaké formě aktivit typu PPP vytvářením speciálních armádních jednotek, se kterými spolupracují odborníci z komerčního i akademického sektoru a údajně i tamější hackerská komunita.

Na stránkách Ministerstva obrany, které obsahují oficiálně sdělované informace o armádě jako takové, se vyskytuje několik zmínek, které se týkají kybernetické války:

- Nejnovější tzv. „bílý sešit“ (bílá kniha) z března 2011 vydaný k nejnovější doktríně národní obrany v roce 2010[39] obsahuje pasáž, že „*národní obrana má za úkol … zajišťovat čínské bezpečnostní zájmy v kosmickém prostoru, elektromagnetickém prostoru a v kybernetickém prostoru*.“[40]

---

[33] Military Power of the People’s Republic of China 2008, Office of the Secretary of Defense, A Report to Congress Pursuant to the National Defense Authorization Act [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.defense.gov/pubs/pdfs/china_military_report_08.pdf>.

[34] Military Power of the People’s Republic of China 2006, Office of the Secretary of Defense, A Report to Congress Pursuant to the National Defense Authorization Act [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.defense.gov/pubs/pdfs/china%20report%202006.pdf>.

[35] FY04 Report to Congress on PRC Military Power Pursuant to the FY2000 National Defense Authorization Act, Annual Report on the Military Power of the People’s Republic of China [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.defense.gov/pubs/d20040528prc.pdf>.

[36] Čínská armáda neprovozuje vlastní web. Oficiální informace o ní lze nalézt na stránkách Ministerstva obrany:
Ministry of National Defense of the People's Republic of China [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://eng.mod.gov.cn/>.
Poznámka: Ministerstvo obrany není nadřízené Čínské lidové armádě. Tu řídí orgán Komunistické strany Číny, jehož název lze přeložit jako „Centrální vojenská komise“.

[37] WANG, Jian-Wei; RONG, Li-Li, Cascade-Based Attack Vulnerability on the US Power Grid [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.sciencedirect.com/science/article/pii/S0925753509000174>.

[38] VENTRE, Daniel, Chinese Information and Cyber Warfare; in: e-International Relations, 13. IV. 2010 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.e-ir.info/?p=3845>.
De WEESE, Steve; KREKEL, Bryan a kolektiv, Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation, 9. X. 2009 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.uscc.gov/researchpapers/2009/northropgrumman_prc_cyber_paper_final_approved%20report_16oct2009.pdf >.

[39] China's National Defense in 2010; in: Ministry of National Defense of the People's Republic of China, 31. III. 2011 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://eng.mod.gov.cn/defensenews/2011-03/31/content_4235452.htm> (**viz snímek z tiskové konference**).

[40] „*China's national defense is tasked to … maintain its security interests in space, electromagnetic space and cyber space …*“ a dále: „*Čínská lidová armáda zintenzivňuje teoretické studie o společných operacích za předpokladů informatizace, pokročilého rozvoje high-tech zbraní a vybavení, vyvíjí nové typy bojových prostředků ….*“ („*The PLA intensifies theoretical*

- Krátký článek nadepsaný „Vojenští experti sdílejí názory na „kybernetickou obranu“ a národní obranu“ obsahuje[41] mj. následující tvrzení: „*… kybernetická obrana“ by měla být považována za důležitou součást národní obrany … stát by měl ustanovit vojensko-civilní mechanismus pro sdílení informací o hrozbách v kyberprostoru … koordinaci útočných a obranných akcí …*“. „*Konflikt v kyberprostoru se stal novým typem války mezi státy.“ „Čínská armáda nemá jinou možnost … . V tom spočívá důležitý a základní projekt: vytvořit mocnou armádu pro bitevní pole v kyberprostoru.*“
- Tamější vojenští experti ovšem zároveň dosud zásadně popírali[42] tvrzení, že by země vyvíjela prostředky kybernetické války a tvrdí, že „*spojovat hackerské kybernetické útoky s čínskou vládou bylo bezdůvodné.*“[43] V nejnovější době je opět možno identifikovat jakýsi posun i v této oblasti a koncem května tohoto roku mluvčí armády oznamil[44] zřízení armádní „jednotky kybernetické bezpečnosti“, která by měla chránit stát proti kybernetrickým útokům. Citovaný článek, který tuto informaci uvádí, však velmi příhodně tuto zprávu komentuje upozorněním na důležitou skutečnost, že v čínském pojetí může být kybernetická válka vedena nejen proti vnějšímu nepříteli, ale ve stejné míře i proti vlastním občanům (ve formě získávání zpravodajských informací a blokování některých stránek a služeb, jako jsou Twitter a Facebook).

Podrobnější informace o armádních složkách, které mají co do činění s kybernetickou válkou, lze nalézt porůznu v otevřejných zdrojích. Situaci poměrně podrobně srhnuje již citovaná zpráva,[45] kterou pro potřeby americké vlády vypracovala společnost Northrop Grumman. Hlavní roli hraje třetí a čtvrté oddělení Generálního štábu čínské armády a dále armádní tzv. „technické průzkumné úřady“.

- 4. oddělení Generálního štábu je v amerických zdrojích označováno za oddělení elektronických protiopatření. Různé zdroje naznačují, že právě toto oddělení má hlavní autoritu v ofenzívní informační válce.
- 3. oddělení Generálního štábu je technicky i personálně velmi rozsáhlé (údajně má mít více než 130 000 pracovníků), protože má na starosti čínské stanice radiového zpravodajství (*SIGINT*). Provádí patrně i různé další formy odposlechů, včetně potřebných analýz.
- Technické průzkumné úřady. Po teritoriu státu je rozmístěno šest těchto úřadů, které jsou zodpovědné za sběr dat pro radiové zpravodajství se zaměřením na „taktické a strategické cíle“. O jejich podřízenosti a činnosti je známo jen málo. Třetí průzkumný úřad měl například provádět „výzkum v teoriích informační války“.

---

studies on joint operations under conditions of informationization, advances the development of high-tech weaponry and equipment, develops new types of combat forces, …“).

[41] DONGMEI, Ouyang, Military Experts Share Views on “Cyber Defense” and National Defense; in: Ministry of National Defense of the People's Republic of China, 6. I. 2011 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://eng.mod.gov.cn/Opinion/2011-01/06/content_4217899.htm>.

[42] DONGMEI, Ouyang, Chinese Experts Rebute Pentagon Cyber Report; in: Ministry of National Defense of the People's Republic of China, 18. VIII. 2010 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://eng.mod.gov.cn/Opinion/2010-08/18/content_4185232.htm>.

[43] JIE, Chen, Linking Hackers' Cyber Attacks with Chinese Government, Military Groundless: Defense Spokesman; in: Ministry of National Defense of the People's Republic of China, 25. II. 2010 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://eng.mod.gov.cn/DefenseNews/2010-02/25/content_4126562.htm>.

[44] BEECH, Hannah, Meet China’s Newest Soldiers: An Online Blue Army; in: Time World, 27. V. 2011 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://globalspin.blogs.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/>.

[45] De WEESE, Steve; KREKEL, Bryan a kolektiv, Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation, 9. X. 2009 [online; citováno 14. VI. 2012]. Dostupné z WWW: <http://www.uscc.gov/researchpapers/2009/northropgrumman_prc_cyber_paper_final_approved%20report_16oct2009.pdf>.