Josef Mrázek

MEZINÁRODNÍ PRÁVO V KYBERNETICKÉM PROSTORU

Abstrakt: *Počet různých kybernetických operací v kybernetickém prostoru včetně kybernetických útoků roste. Kybernetické hrozby představují závažná rizika jak pro státní, tak i soukromý sektor a některé z nich mohou ohrozit kybernetickou bezpečnost jednotlivých států a případně i mezinárodní bezpečnost jako celek. Kybernetické útoky tvoří různé činy narušující, omezující nebo ničící počítače a počítačové sítě. V těchto případech lze některé kybernetické útoky zřejmě přirovnat k ozbrojenému útoku ve smyslu čl. 51 Charty OSN. Existuje silná tendence k vojenskému řešení kybernetické bezpečnosti. NATO vyvíjí způsobilost a možnosti ke kybernetickému vedení války na novém „bojišti". USA vytvořily Kybernetické velení jako součást své vojenské strategie. Tato studie se zabývá kybernetickou bezpečností, kybernetických útokem a kybernetickými zločiny a všímá si i nejednotné interpretace kybernetických pojmů. Jedinou mezinárodní úmluvou je v tomto ohledu Evropská úmluva o kybernetickém zločinu. Podle názoru autora každá činnost v kybernetickém prostoru musí být v souladu s mezinárodním právem, i když speciální mezinárodní normy zatím neexistují. Základním tématem práce je, kdy kybernetický (počítačový) útok může představovat použití ozbrojené síly (casus belli), které se může rovnat „ozbrojenému útoku", vyvolávajícímu právo na sebeobranu podle čl. 51 Charty OSN.*

Klíčová slova: *kybernetické operace, kybernetický útok, kybernetická bezpečnost, kybernetický zločin, kybernetický prostor, kybernetické válčení*

ÚVOD

Pojmy „kybernetická hrozba" (*cyber threat*), „kybernetický útok" (*cyber attack*), „kybernetická bezpečnost" (*cyber security*), „kybernetický prostor" (*cyber space*), „kybernetický zločin" (*cyber crime*), „kybernetický terorismus" (*cyber terrorism*) nebo dokonce pojmy jako „kybernetická válka" (*cyber war*), „kybernetické vedení války" (*cyber warfare*), „kybernetická agrese" (*cyber aggression*) a „kybernetická obrana" (*cyber self-defense*), jakož i jiné pojmy spojené s „*cyber*" se staly v posledních letech nedílnou součástí mezinárodněpolitického slovníku.[1] Problematika využívání kybernetického prostoru a počítačů přináší s sebou především celou řadu technických a také bezpečnostních problémů. Stranou nemůže zůstat u těchto otázek ani úprava právní a specificky úprava mezinárodněprávní. I když mezinárodněprávní regulace kybernetických problémů je doposud nedostatečná a málo efektivní, v odborné literatuře se již hovoří o „mezinárodním právu kybernetického prostoru" a obecně i o úloze práva v tomto prostoru.[2]

[1] AMOROSO, E. *Cyber Attack: Protecting National Infrastructure.* Butterworth – Heinemann, 2010; BAYUK, J. L. – HEALEY, J. – ROHMEYER, P. – SACHS, M. H. – SCHMIDT, J. – WEISS, J. *Cyber Security Policy Guidebook.* John Wiley & Jons, 2012; CARR, J. *Inside Cyber Warfare.* O'Reilly Media, 2009; CLARKE, R. A. *Cyber War.* HarperCollins, 2010; CLARKE, R – KNAKE, R. A. *Cyber War: The Next Threat to National Security and What to Do About It.* Ecco, 2012; DINNIS, H. – HARRISON. *Cyber Warfare and the Laws of War.* Cambridge University Press, 2012; ENGHELBERG, H. – TENZER, G. *The Evolution of Cyber Terrorism: A Precision – Delivery Weapon, An Asymmetric War, Cyber Attacks.* The New Frontier, 2011; HEATHER, H. D. *Cyber Warfare and the Laws of War.* Cambridge University Press, 2012; ROSENBERG, P. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World.* Praeger, 2013; SHACKELFORD, SCOTT J. *Managing Cyber Attack in International Law, Businnes and Relations: In Search of Cyber Peace.* Cambridge University Press, 2013; VENTRE, D. *Cyberattaque et Cyberdéfence.* Hermes-Lavoisier, 2011.

Celkem běžně se lze setkat již i s pojmem „kybernetický právník“ (*cyber lawyer*).[3] Jde o pojem, který zřejmě vystihuje specializovaného právníka, který ovládá alespoň rámcově i kybernetickou technologii. Mezinárodní encyklopedie kybernetického práva zahrnuje části věnované „kybernetickému právu Evropské unie“ nebo „mezinárodnímu a globálnímu telekomunikačnímu právu“ a obsahuje i „kodex kybernetického práva“ nebo texty kybernetických zákonů vybraných zemí, které se budou postupně rozšiřovat.[4] I v České republice se již objevují publikace věnované kybernetickému právu.[5]

Na řadě univerzit se dnes vyučuje „kybernetické“ nebo také „internetové“ právo. Na Harvardu např. existuje Berkmanovo středisko pro internet a společnost. V rámci Harvard Law School působí i tzv. kyberneticko-právní klinika (*Cyber law clinic*), která poskytuje vysoce kvalifikované právní služby vládním entitám, neziskovým organizacím i jednotlivcům a napomáhá studentům při přípravě pro jejich „high-tech“ praxi. Služby „kliniky“ jsou využívány v různých oblastech právní praxe, jako jsou legislativa, řešení soudních sporů a advokátní činnost.[6] Výzkumem „mezinárodního práva kybernetického prostoru“ se zabývá i další prestižní univerzita v Georgetownu[7] nebo Institut OSN pro odzbrojení (UNIDIR).[8] Výzkum a studium kybernetického práva se neomezuje pouze na americké nebo evropské vysoké školy, nýbrž se prosazuje i v Asii a na dalších kontinentech.[9]

Kybernetické hrozby pocházejí od států i soukromých subjektů. Problémem zatím často zůstává i identifikace místa (země) odkud kybernetické hrozby a útoky pocházejí. Komplikované je i přesné vymezení samotných kybernetických útoků a jejich odlišení od pouhých kybernetických „incidentů“ nebo kybernetické „exploatace“. Kybernetické operace proti internetu napadají vojenské, bezpečnostní a zpravodajské servery s cílem narušit bezpečnostní, ekonomickou, finanční a komunikační činnost státních i soukromých institucí. Internetem se rozumí internetová síť spojující mnohé počítačové sítě a spočívající na společném adresném systému a komunikačním protokolu nazývaném *Transmission Control Protocol* (ACP/IP). Internet byl vytvořen v roce 1983 a má svůj počátek v programu ARPANET (Advanced Research Projects Agency Network) Ministerstva obrany USA z roku 1969. Jeho cílem bylo zajistit bezpečnou komunikační síť. Později se výzkumem a vytvořením podobných paralelních sítí v USA zabývala

---

2 DUMORTIER, J. *International Encyclopaedia for Cyber Law.* www.IELaws.com; Webster's New World Hacker Dictionary, Webster's New World, 2006.

3 http://askacyberlawyer.com/2011/06/07/a-call-for-international-cyber-law/; What is cyberlawyer, viz http://www.webopedia.com/TERMIC/cyberlawyer.html: „term used to describe a lawyer who is an expert on the law as it relates to online communications“.

4 DUMORTIER, Jos. (ed.), op. cit. 2. K právním předpisům evropských zemí viz např. VALERI, L. – SOMMERS, G. – ROBINSON, N. – GRAUX, H. – DUMORTIER, J. *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*, publikovanou v rámci RAND Corporation pro potřeby Evropské komise v roce 2006, RAND Europe URL: http://www.rand.org/randeurope.

5 POLČÁK, R. – ČERMÁK, J. – LOEBL, Z. – GŘIVNA, T. – MATEJKA, J. – PETR, M. *Cyber Law in the Czech Republic.* Kluver Law International, 2012.

6 www.cyberlaw.harvard.edu/teaching/cyberlawclinic.

7 International Cyberspace Law Research, www.georgetown.edu/library/research/guides/cyberspace.cfm.

8 Cyberwarfare and International Law UNIDIR 2011, www.isn.ethz.ch/digital-library/publications/detail/?/ng=en&id=134218.

9 Viz např. www.asvanlaws.org/index.php/UbRDMnOfg, Diploma in Cyberlaw; International Cyber Law Research Center at Naavi's Cyber Law Colleage, www.ilze.org.

The National Science Foundation (NSF) a to právě s využitím technologií ARPANET.[10] Ochrana proti kybernetickým útokům je svěřována vojenským a jiným specializovaným státním institucím. Z mezinárodněprávního hlediska je významnou otázkou, zda některé kybernetické útoky mohou dosáhnout úrovně ozbrojeného útoku ve smyslu čl. 51 Charty OSN, opravňujícího státy k použití ozbrojené síly v sebeobraně. V dokumentech NATO jsou kybernetické útoky označovány za reálnou vojenskou hrozbu, vyvolávající potřebu upevňování kybernetické obrany (*cyber defence*).[11]

Záměrem autora tohoto článku byla orientace především na mezinárodněprávní problémy kybernetických útoků, zejména z hlediska zákazu použití ozbrojené síly v mezinárodních vztazích. Vzhledem k tomu, že v české právnické literatuře zatím neexistuje zpracování problematiky kybernetických operací v dostatečné míře, rozhodl se autor pro širší pojetí své práce a nemohl se proto vyhnout i dílčí popisnosti a interpretaci základních pojmů, které se často i liší. Nelze pominout, že otázky využívání kybernetického prostoru jsou poměrně novým fenoménem, na který právo obecně a mezinárodní právo zvlášť teprve hledá odpovědi a řešení. I když řešení právních otázek kybernetických operací se nerodí ve vzduchoprázdnu. Právní rámec pro potírání kybernetických útoků je stále nedokonalý a fragmentární, jak v oblasti práva vnitrostátního, tak i mezinárodního. Sílí proto oprávněné tendence k vypracování nových právních instrumentů pro řešení kybernetické bezpečnosti. Základem by podle některých názorů měla být komplexní univerzální mezinárodní úmluva, zabývající se mezinárodní spoluprací při zabezpečení kybernetické bezpečnosti a z toho vyplývajícími otázkami právní odpovědnosti a donucení. Přitom však neexistuje všeobecné pozitivní nazírání na potřebu takové smluvní úpravy. Kybernetické útoky a incidenty v mezinárodním životě nebývají jednostrannou ani jednorázovou záležitostí a státy s nimi ve své politice a praxi ve skutečnosti počítají. Je třeba také z právního hlediska vyjasnit otázku, zda vůbec, za jakých okolností a jaké kybernetické útoky mohou být legální. Např. v roce 2011 byl proveden kybernetický útok na íránský jaderný program, jehož důsledkem bylo, že jaderné centrifugy se v Íránu dostaly mimo jeho kontrolu. Útok způsobil počítačový vir nebo „červ" „*Stuxnet*", který byl pravděpodobně společně testován USA a Izraelem v Negevské poušti v izraelském komplexu Dimona.[12]

Obtížnost právní regulace činnosti v kybernetickém prostoru může demonstrovat i následující skutečnost. V červnu 2013 vyšlo najevo, že National Security Agency (NSA) v USA v rámci programu PRISM sleduje internetovou komunikaci z celého světa. Zprávu zveřejnil nejprve britský deník *The Guardian* na základě informací, které vynesl Edward Snowden, technik CIA a spolupracovník NSA. NSA může získávat e-maily, fotografie, videa, soubory dat, videokonference, výpisy aktivit, zprávy ze sociálních sítí i soukromé zprávy. V rámci programu má NSA přístup k údajům takových společností, jako jsou AOL,

[10] *The New Encyclopaedia Britannica*, Vol. 6, Micropaedia, Chicago, London, 2002, s. 354–5.

[11] NATO Agrees on Common Approach to Cyber Defence, April 2008, http://www.euroactiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377. Srov.: „Cyber attack continue to pose a real threat to NATO and cyber defence will continue to be a core capability of the Alliance", www.nato.int/cps/en/natolive/75747.htm.cps/en/SID-E61FF165-78BBC3C8/natolive/topics_78170.htm.

[12] FILDES, J. Stuxnet Worm Targeted High-Value Iranian Assets. *BBC News*, Sept. 23, 2010, http://www.bbc.co.uk/news/technology-11388018; též http://www.economist.com/blogs/babbage/2010/09/stuxnet.worm.

Apple, Google, Microsoft, Paltak, Skype nebo Youtube.[13] Podle informací Snowdena USA od roku 2002 nabourávají čínské počítačové systémy. Jde o delikátní záležitost, neboť USA a osobně prezident Obama kritizují kybernetické útoky přicházející z Číny. Americká firma Mandiant obvinila v únoru 2013 čínskou armádu z provádění hackerských útoků na cíle zejména v USA, ale také ve Velké Británii a Kanadě.[14] Čínská vláda takové aktivity popírá. Oficiální místa USA, včetně NSA a amerického prezidenta, poukazují na to, že program PRISM zmařil desítky teroristických útoků. Podobný program vyvinula Velká Británie a nepochybně i další státy.

Ve strategických plánech USA a NATO se počítá i s koncepcí „kybernetického ozbrojeného útoku". Použití ozbrojené síly v sebeobraně proti kybernetickým útokům je považováno za nedílnou součást „komplexní strategie kybernetické bezpečnosti" spolu s dalšími komponenty, včetně lepší „síťové bezpečnosti" a „ofenzivních kybernetických opatření".[15]

Kybernetický útok většinou nemá znaky útoku, působícího „fyzické" škody. Jasný konsensus týkající se povahy určitého kybernetického útoku, jako útoku „ozbrojeného", neexistuje. Menšinově se v literatuře vyskytl i názor, že kybernetický útok nemůže představovat „ozbrojený útok".[16] Podle opačného názoru může i některý kybernetický útok představovat ozbrojený útok v závislosti na jeho fyzických účincích. Tento *effect-based approach* vychází z toho, že i kybernetický útok může mít stejné nebo i horší účinky jako použití konvenčních bomb a nábojů. Mezi příklady takových účinků se obvykle uvádějí zničení vodních děl a přehrad nebo exploze letadel atp. pomocí počítačových sítí.[17]

Bylo by jistě účelné a užitečné nejprve precizněji objasnit základní kybernetické pojmy, což je poměrně obtížné. Tyto pojmy a definice se u jednotlivých autorů a institucí často liší. Není snadné dosáhnout obecnějšího konsensu a odstranit existující terminologický a obsahový zmatek. Nebezpečí spočívající ve zneužití nových informačních a komunikačních technologií nepochybně existuje jak v civilní, tak i ve vojenské sféře, což úzce obecně souvisí s otázkami národní i mezinárodní bezpečnosti, nejen tedy s otázkami kybernetické bezpečnosti v úzkém slova smyslu.

1. K POJMŮM KYBERNETICKÉ BEZPEČNOSTI A KYBERNETICKÝCH ÚTOKŮ

Počítače a počítačové sítě, které je spojují, vytvářejí respektive představují kybernetický prostor. Využívání kybernetického prostoru se dotýká prakticky všech oblastí života

[13] Prism Collection Details, http://technet.idnes.cz/nsa-fbi-sledovani-prism.usa-soukromi-data-/sw_internet.aspx.

[14] http://zpravy.tiscali.cz/potvrzeno-cina-soustavne-provadi-hackerské-utoky-po-celem-svete.

[15] WAXMAN, M. C. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. Naval War College, *International Law Studies*. 2013, s. 110.

[16] K různým názorům na tuto otázku viz např. HATHAWAY, O. A. – CROOTOF, R. – LEVITZ, PH. – NIX, H. – NOWLAN, A. – PERDUE, W. – SPIEGEL, J. The Law of Cyber Attack, *California Law Review*. Vol. 100, Issue 4, s. 817, 841–9.

[17] DINSTEIN, Y. Computer Network Attacks and Self-Defense. In: M. S. Smitt – B. T. O'Donnell (eds). U.S. Naval War College *International Law Studies*. Vol. 76, 2002, s. 119.

moderní společnosti. Kybernetická bezpečnost každého států hraje mimořádně významnou roli v současném globalizovaném světě. Kybernetický prostor nebo také „doména" (*domain*) se podle expertů skládá ze tří vrstev: 1) fyzické, 2) syntaktické, 3) sémantické. Fyzická část zahrnuje hardware, kabely, satelity a jiná vybavení. Syntaktická část se skládá z počítačových operačních systémů a jiného softwaru. Sémantická vrstva pak zahrnuje vzájemné působení lidského činitele a informací získaných z počítačů, jejich vyhodnocení a využití uživatelem.[18]

Kybernetické útoky pak mohou směřovat proti všem nebo i jednotlivým vrstvám kybernetického prostoru. Útoky jsou vedeny kybernetickými prostředky (hovoří se také o „kybernetických zbraních"), které ničí, paralyzují, monitorují nebo jinak poškozují počítačový software. Za takové kybernetické zbraně jsou označovány závadné softwary nebo závadné komponenty jako jsou viry, trojské koně a špionážní zařízení nebo počítačové „červy". Sémantické kybernetické útoky mají ovlivnit percepci a vnímání počítačových dat a jejich cílem je získání citlivých údajů jako jsou přístupové kódy, hesla nebo finanční údaje (*phishing*, *pharming*). Využívají se přitom podvodné e-maily zasílané uživatelům počítačů, žádající o zaslání údajů ze zdánlivě legitimních důvodů. Jde většinou o trestnou činnost a počítačovou špionáž.

Velkým problémem a velkou výzvou pro ochranu kybernetické bezpečnosti je zřejmě stávající anonymita a obtížnost odhalení autorů kybernetických útoků. Obrana proti kybernetickým útokům zahrnuje *firewalls* pro filtrování síťové komunikace, šifrování dat, nástroje na obranu a odhalení sítě narušitelů, fyzickou bezpečnost zařízení a vybavení, jakož i monitorování uživatelských sítí. Pokud jde o obranu proti kybernetickým útokům, hovoří se o „vrstvené aktivní a pasivní obraně". Státy se většinou omezují na defenzivní obranu z obavy, že aktivní obrana porušuje válečné právo. Aktivní kybernetickou obranou se pak rozumí elektronické opatření, které omezuje počítačovou obranu „protivníka" na pasivní. Právo k aktivní obraně vyplývá pak z povinnosti států zabránit nestátním aktérům využívat jejich území ke spáchání útoků.

Existují různé definice kybernetické bezpečnosti i dalších kybernetických pojmů. Kybernetická bezpečnost je stručně definována např. jako stav ochrany proti kriminálnímu nebo neoprávněnému použití elektronických údajů nebo opatření přijatá k dosažení jejich ochrany.[19] Podle jiné stručné definice se jedná o opatření přijatá na ochranu počítačů a počítačových systémů.[20] Kybernetická bezpečnost je definována i jako „soubor technologií, procesů a praxe určený k ochraně sítí, počítačů, programů a dat před útokem, poškozením nebo neoprávněným přístupem".[21] Za zmínku stojí i definice vypracovaná Světovou telekomunikační unií. Podle této definice se kybernetickou bezpečností rozumí nástroje, politiky, bezpečnostní koncepce, bezpečnostní záruky, pokyny,

[18] SHELDON, John B. Cyberwarfare: The Invisible Threat. *Encyclopaedia Britanica*, 2011, Book of the Year, s. 182–183; též např. HATHAWAY, O. A., op. cit. 16, s. 860, lehce modifikovaný článek viz http://scholarship.law.berkeley.edu/california/law/review, s. 12–13.

[19] Srov. „…the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this"; viz např. Oxforddictionaries.com/definition/cybersecurity.

[20] Srov. „measures taken to protect a computer or computer system", Meriam Webster Dictionary, www.meriam-webster.com/dictionary/cybersecurity.

[21] Srov. „cybersecurity is the body of technologies, processes and practices designed to protect networks, computers programs or unauthorized access", www.whatis.techtarget.com/definitions/cybersecurity.

rizikový management, přístupy, akce, výchova, směrnice, záruky a technologie, které mohou být použity na ochranu kybernetického prostředí a organizace a aktiv uživatele.[22] V českém Výkladovém slovníku kybernetické bezpečnosti, vydaném Policejní akademií ČR a českou pobočkou AFCEA, je „kybernetická bezpečnost" (*cyber security*) zmiňována vedle „počítačové bezpečnosti" (*computer security*), i když jde v podstatě o synonyma. Zatímco prvním pojmem autoři míní „souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru", druhý pojem označují za „obor informatiky, který se zabývá zabezpečením informací v počítačích". Počítačová bezpečnost podle slovníku zahrnuje ochranu proti: 1) neoprávněné manipulaci se zařízením počítačového systému; 2) neoprávněné manipulaci s daty; 3) krádeži (nelegálnímu pořizování kopií dat) nebo poškození; 4) narušování bezpečné komunikace a přenosu dat (kryptografie); 5) poškozování bezpečného uložení dat a 6) poškozování dostupnosti, celistvosti a nepodvrhnutelnosti dat.[23]

Kybernetická nebo také počítačová bezpečnost se v úzkém slova smyslu chápe jako technologie a postupy určené k ochraně počítačů, počítačových sítí a údajů před neoprávněným přístupem, zranitelností a útoky spáchané kybernetickými zločinci. Existují i určité technické normy např. ISO 27001 a ISO 27002 jako standardy kybernetické bezpečnosti pro vytváření, implementaci, operační činnost, monitorování, udržování, revizi a zlepšování managementu, bezpečnostního a informačního systému.[24] Kybernetická bezpečnost se vztahuje k technologii a prostředkům ochrany počítačů, počítačových sítí a dat před neoprávněným přístupem a internetovou zranitelností. Jedná se o technický problém a může jít i o strategický koncept, neboť některé kybernetické útoky mohou ohrozit národní i mezinárodní bezpečnost.

Kybernetickou bezpečností se zabývá Agentura EU pro bezpečnost sítí a informací (ENISA), která poskytuje své služby a expertízy Komisi EU i jednotlivým členským státům. Cílem je zvýšit úroveň síťové a informační bezpečnosti veřejného i soukromého sektoru a též občanů.[25] ENISA má sídlo v Heraklionu na Krétě. Problematice informační bezpečnosti internetu je věnován např. i zvláštní oddíl ve Zprávě zvláštního zpravodaje VS OSN Franka La Rue o podpoře a ochraně práva na svobodu názoru a projevu novinářů.[26]

S kybernetickou bezpečností úzce souvisí pojem kybernetického útoku. V širším významu je za kybernetický útok označována (nepřesně) jakákoli akce proti počítačové síti, včetně získávání citlivých údajů (kódy, hesla) a počítačové špionáže. V užším významu

---

[22] Srov. „Cyber security is the collection of tools, policies, security concept, security safeguards, guidelines, risk management, approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets", www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[23] JIRÁSEK, P. – NOVÁK, L. – POZÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní Akademie ČR v Praze, Česká pobočka AFCEA, 2013, s. 57 a 72.

[24] Srov. „ISO 27001 (The Cyber Security Standard), ISO 27001 Toolkit, ISO 27002/Infosec-e-Learning; ISO 27001 is part of the ISO 27002 family of international information security standards", http://www.webopedia.com/TERMIC/cybersecurity.aspx.

[25] http://www.enisa.europe.eu/about-enisa; k zaměření činnosti ENISA viz nařízení EU č. 526/2013 Evropské komise a Rady z 21. 5. 2013, které nahradilo původní nařízení č. 466/2004 z 10. 3. 2004.

[26] Report of the Special Repporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, Doc. UNGA A/HRC/20/17 ze 4. 6. 2012, s. 11.

pak kybernetické útoky běžnou počítačovou trestnou činnost a průmyslovou špionáž nezahrnují. Kybernetický útok v užším respektive pravém slova smyslu je obvykle definován jako každá akce podniknutá ke zničení nebo poškození funkcí počítačových systémů a počítačové sítě z politických nebo bezpečnostních důvodů.[27] Někdy dochází i ke ztotožňování různých kybernetických „incidentů" s kybernetickými útoky nebo běžnými kybernetickými zločiny. Odpověď na otázku, zda např. počítačové viry vyřazující z provozu banky, trhy s cennými papíry, letecké a námořní systémy nebo provoz jaderných a jiných elektráren, jsou kybernetickými útoky, není vždy snadná. Nejširším všezahrnujícím pojmem kybernetické činnosti jsou zřejmě „kybernetické operace".

Podle Národní výzkumné rady USA (The U.S. National Research Council) lze kybernetické útoky chápat jako „záměrné akce směřující ke změně, zničení, oklamání, znehodnocení nebo zničení počítačových systémů nebo informací a programů v těchto systémech nebo sítích obsažených nebo je přenášejících".[28] Široce vymezují kybernetický útok někteří američtí autoři, kteří jím rozumí „jakoukoli akci – *hacking*, bombardování, vystřižení údajů, infikování počítačové sítě atd. – jejímž cílem je poškodit nebo zničit funkce počítačové sítě".[29] Kybernetický útok se definuje většinou podle jeho cíle, nikoli podle použitých prostředků. Použití kybernetické sítě v Nevadě pro řízení bezpilotních letadel k útoku na cíle v Pákistánu nebo jinde není podle některých názorů kybernetickým útokem, zatímco použití výbušnin k poškození podmořských kabelů pro přenášení informací mezi kontinenty takovým kybernetickým útokem je. Autoři se přitom odvolávají na „národní vojenskou strategii USA pro kybernetické operace" z roku 2006, která ztotožnila kybernetické útoky se strategií v „ofenzivních kybernetických operacích".[30]

Pod kybernetické útoky jsou autory citované studie řazeny v širokém slova smyslu rozdílné činnosti. Jsou k nim řazena např. distribuovaná odepření služby (*distributed denial of service* – DDOS). Jde o využití koordinovaných *bootnets*, tj. tisíců „zombie" počítačů ovládaných zákeřnými počítačovými viry, které přetíží servery systematickými návštěvami určitých webových stránek. Na podobném principu funguje útok DOS představující nedistribuované odmítnutí služby (*denial of service*). Dochází zde rovněž k zahlcení serverů obrovským množstvím požadavků, nejde však o distribuovaný útok a nejsou využívány zotročené počítače. Útok DOS je veden z jednoho centra. Dalším útokem je např. šíření nepřesných informací (*planting inaccurate informations*). Jde o sémantický útok, který je více sofistikovaný než DDOS. Počítačový systém po takovém

[27] „A cyber-attack consists of any action taken to undermine the function of a computer network for a political or national security purpose"… „A cyber-attacks means can include any action-hacking, bombing, cutting, infecting and so forth – but the objective can only be to undermine or discrupt the function of a computer network"; Hathaway et al. op. cit. 16, s. 826–830.

[28] Srov.: „Deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or network or the information and/or programs resident in or transiting these systems or networks", the U.S. National Research Council, Technology, Policy Law and Ethics Regarding U.S. Acquisition and use of cyberattack capabilities, 2009, viz HATHAWAY et al., op. cit. 16, s. 826–827.

[29] Ibid.

[30] „Using a computer network in Nevada to operate a predator drone for a kinetic attack in Pakistan is not a cyber-attack; rather, it is technologically advanced conventional warfare. Using a regular explosive to sever the undersea network cables that carry the information packets between continents, on the other hand, is a cyber-attack. This view is consistent with that offered by the U.S. Department of Defense, which has identified kinetic attack as a strategy in „cyber offensive operations"." Ibid., s. 11.

útoku působí zdánlivě normálně. Jiným druhem kybernetických útoků je infiltrace do zabezpečného počítačového systému (*infiltrating a secure computer network*). Po infiltraci může pachatel uskutečnit různé destrukční akce nad rámec pasivní kybernetické špionáže, která se většinou za kybernetický útok neoznačuje.[31] Syntaktické útoky narušují operační počítačové systémy a mají za následek poškození počítačové sítě. Sémantické útoky zachovávají operační počítačový systém, který zdánlivě funguje správně, generuje však nesprávné informace a nesprávné odpovědi.

Na rozdíl od „kybernetických útoků" pak „kybernetické exploatace" či „kybernetické vykořistění" (*cyber exploitations*) podle týchž autorů nepředstavuje žádné narušení počítačové sítě, nýbrž se omezuje pouze na monitorování, kopírování dat a špionáž pomocí počítačového systému. Příkladem může být krádež bankovních dat, kódů bankovních karet, narušování obchodního tajemství nebo zjišťování vojenských, bezpečnostních a jiných informací z počítačového systému. Kybernetickým útokem tak není pouhé snížení bezpečnosti počítačové sítě v důsledku aktivit, jako jsou špionáž nebo využití cizí počítačové sítě, kopírování jejích dat nebo pasivní pozorování sítě, atp., neboť tato činnost nepůsobí změny, které by ovlivňovaly současnou nebo i budoucí schopnost počítačových sítí správně fungovat. Politická nebo průmyslová kybernetická špionáž nejsou většinou považovány za kybernetické útoky, nýbrž za „pouhé" kriminální činy.[32]

2. KYBERNETICKÉ ZLOČINY

Kybernetickým zločinem se rozumí každý kriminální čin proti počítačům a počítačovým sítím. Kybernetickým zločinem je i každý trestný čin spáchaný pomocí internetu, jako jsou zločiny spáchané z nenávisti, telemarketingové a internetové podvody, zcizení identity nebo krádež dat z kreditní karty. Kybernetické zločiny zahrnují širokou škálu použití počítačových prostředků (*computer based means*) k páchání nelegálních činů. Jednotně přijímaná definice kybernetického zločinu rovněž neexistuje. Nejčastěji se jedná o podvodnou činnost na internetu, internetové pirátství, přechovávání a sdílení dětské pornografie a nelegální pronikání do počítačů. Kybernetické zločiny nemají většinou politické nebo bezpečnostní cíle a nenarušují fungování počítačové sítě.

Jsou to právě politické nebo národně bezpečnostní motivy, které jsou rozhodující pro rozlišení závažných kybernetických útoků od běžných kybernetických zločinů. Agresivní akce podniknutá státním aktérem je pak většinou kybernetickým útokem. Stejně tak i určitý kybernetický zločin spáchaný nestátním aktérem z politických nebo národně bezpečnostních důvodů může být zřejmě rovněž kybernetickým útokem. Kybernetické zločiny, které nejsou spáchány z důvodů politických nebo bezpečnostních jako např. internetové podvody, krádeže identity, pirátství v oblasti průmyslového vlastnictví atp., nesplňují požadavek kybernetického útoku a zůstávají proto pouhými kybernetickými

[31] Ibid., s. 839.

[32] Srov. „More cyber-espionage or cyber-exploitation does not constitute a cyber-attack, because neither of these concepts involves altering computer networks in a way that affects their current or future ability to function." The CIA emphasizes that cyber-espionage does not fall under the umbrella of cyber-warfare, likely because the U.S. government – like many other governments – routinely engages in espionage „over communications networks…", ibid., s. 830.

zločiny.[33] V České republice bylo vyšetřování kybernetických zločinů svěřeno mimo jiné i Oddělení informační kriminality Úřadu služby kriminální policie a vyšetřování na Policejním prezidiu Policie ČR.

Úmluva Rady Evropy o kybernetických zločinech přijatá Radou Evropy dne 23. listopadu 2001 v Budapešti (vstoupila v platnost 1. 7. 2004) zahrnuje široký okruh trestných činů spáchaných pomocí počítače. Jedná se o protiprávní činnost proti důvěrnosti předávaných zpráv, integritě a použitelnosti počítačových systémů, sítí, počítačových dat, jakož i zneužití takových systémů, sítí a dat.[34] Úmluva obsahuje základní směry mezinárodní spolupráce při potírání této činnosti. Již v preambuli členské státy jako svou prioritu vytyčily „společnou trestní politiku", zaměřenou na ochranu společnosti proti kybernetickému zločinu, *inter alia* na základě přijetí odpovídající národní legislativy a rozvoje mezinárodní spolupráce. Cílem úmluvy je odvrátit pachatele od akcí zaměřených proti řádnému fungování počítačových systémů a sítí, jakož i zabránit zneužití těchto systémů sítí a dat na základě kriminalizace uvedeného chování na národní i mezinárodní úrovni. Úmluva má usnadnit odhalování, vyšetřování i stíhání těchto činů. Úmluva v čl. 1 obsahuje definice termínů, jako jsou „počítačový systém", „počítačová data", „poskytovatel služeb" a „komunikační údaje". Články 2 až 10 se týkají jednotlivých počítačových zločinů. Články 11 až 13 se zabývají otázkami odpovědnosti. Další články jsou věnovány ochraně počítačových dat, otázkám jurisdikce, vzájemné spolupráce států a konzultací. Úmluva má celkem 48 článků. Každá smluvní strana se zavázala přijmout zákony a jiná opatření, která mohou být nezbytná pro vytvoření jurisdikce ke stíhání zločinů podle čl. 2 až 10 Úmluvy: a) na území smluvní strany; b) na lodi plující pod její vlajkou nebo; c) na palubě letadla registrovaného podle zákonů této strany; d) zločinů spáchaných některým z jejich příslušníků, pokud je zločin trestný podle trestního práva země, ve které byl spáchán nebo byl-li spáchán mimo územní jurisdikci všech států. Dojde-li mezi smluvními stranami ke sporu o jurisdikci, Úmluva předpokládá konzultace, které by měly určit nejvhodnější jurisdikci ke stíhání těchto zločinů (čl. 22). Účelem Úmluvy je doplnění existujících mnohostranných nebo bilaterálních smluv nebo ujednání, včetně Evropské úmluvy o vydávání (sdělení č. 549/1992), Evropské úmluvy o vzájemné pomoci v trestních věcech z 20. 4. 1959 a Dodatkového protokolu ze 17. 3. 1979 k téže úmluvě (čl. 39). Úmluvu Rady Evropy o kybernetickém zločinu podepsalo čtyřicet šest států a dvacet šest států, včetně České republiky, ji ratifikovalo. Úmluva je otevřena podpisu i nečlenským státům Rady Evropy. Na jednání participovaly a smlouvu podepsaly USA, Kanada, Japonsko a Jižní Afrika. Spojené státy Úmluvu také ratifikovaly. Byl již přijat i Dodatkový protokol k této Úmluvě, který se týká činů rasistické a xenofobní povahy, spáchaných prostřednictvím počítačových systémů. Protokol byl otevřen

[33] What is cyber crime? A word definition, from Webopedia Computer Dictionary, http://www.webopedia.com/TERM/cyber_crime.html; srov. „A political or national security purpose distinguishes cyber-attack from simple cyber-crime." Any aggressive action taken by a state actor in the cyber-domain necessarily implicates national security and is therefore a cyber attack whether or not it rises to the level of cyber-warfare. Cyber-crime committed by a non-state actor for a political or national security purpose is a cyber attack."; „Most cyber-crimes do not…constitute cyber-attack or cyber-warfare…some cyber-attacks are neither cyber-crimes not cyber-warfare", též Hathaway et col., op. cit. 16, s. 830–833.

[34] Council of Europe, ETS No 185, Convention on Cyber-crime, Budapest, Nov. 23, 2001, viz http://conventions.coe.int/Treaty/html/185.htm.

k podpisu 28. 1. 2003 a vstoupil v platnost 1. 3. 2006.[35] Kybernetických zločinů se dále týká i Úmluva Rady Evropy o ochraně dětí před sexuálním zneužíváním, která byla vystavena k podpisu 25. 10. 2007 a vstoupila v platnost 1. 7. 2010.[36] Kybernetickými zločiny jsou podle Úmluvy o kybernetických zločinech činy, které jsou trestné podle vnitrostátního nebo mezinárodního práva.

Řada autorů se nyní vyslovuje pro přijetí univerzální mezinárodní úmluvy o posílení kybernetické bezpečnosti a potírání mezinárodních zločinů. Existují však i skeptické hlasy popírající smysl a efektivitu takové budoucí mezinárodní úmluvy. Hlavní námitkou je obtížnost verifikace původce kybernetických útoků. Kromě toho státy nejsou ochotny se předem vzdát možnosti využívat kybernetický prostor ke svému prospěchu nebo se vzdát svých kybernetických operací. Návrh univerzální mezinárodní úmluvy o kybernetickém zločinu a terorismu např. vypracovali již v dubnu 2000 v USA společně pracovníci Standford University, Hoover Institution, The Consortium for Research on Information security and policy (CRISP) a The Center for International Security and Cooperation (CISAC). Tento soukromý návrh zdůrazňoval, že informační infrastruktura je ve zvýšené míře vystavena útokům kybernetických zločinců, že kybernetický zločin je převážně nadnárodní a bude často zahrnovat jurisdikční nároky více států. Je proto podle autorů nutné uzavřít dohody týkající se jurisdikce a donucovacích opatření, které by bránily jurisdikčním konfliktům. Výsledkem standfordské konference byla publikace, která se podrobně zabývá důvody pro vypracování mezinárodní úmluvy pro zvýšení bezpečnosti před kybernetickým zločinem a terorismem.[37] Mezi důvody pro uzavření smlouvy autoři uváděli: kybernetický zločin je nadnárodní a vyžaduje nadnárodní odvetu; kybernetičtí zločinci využívají nedostatků v zákonech a v donucovací praxi států, vystavujíce tak ostatní státy nebezpečí, které jde nad rámec jejich možností jednostranně nebo bilaterálně reagovat; rychlost a technická komplexnost kybernetických aktivit vyžaduje předem připravené a dohodnuté postupy spolupráce při vyšetřování a reagování na hrozby a útoky. Úmluva by měla zajistit, aby všechny strany úmluvy: 1) přijaly zákony, které označí nebezpečné kybernetické aktivity za trestné; 2) tyto zákony vynucovaly nebo vydávaly pachatele k trestnímu stíhání; 3) spolupracovaly při vyšetřování trestné činnosti a vzájemně si poskytovaly důkazy o takové činnosti, participovaly na vypracování a implementaci dohodnutých standardů ke zvýšení kybernetické bezpečnosti. Návrh také předpokládal vytvoření zvláštní mezinárodní agentury jako fóra pro mezinárodní diskusi s ohledem na technologický vývoj a také pro technickou pomoc rozvojovým zemím. Autoři věnovali značnou pozornosti i kybernetickým aktivitám v soukromé sféře. Rychlý vývoj v oblasti kybernetických technologií a operací označili přímo za „kybernetickou revoluci" (*the cyber revolution*).

Pro uzavření univerzální mezinárodní úmluvy se v posledních letech vyslovila řada autorů. Proti uzavření se uvádí rovněž celá řada argumentů. Patří k nim tvrzení, že je obtížné posoudit útoky na jisté hodnoty nebo cíle jako trestné činy nebo válečné zločiny

[35] Additional protokol to the Convention on cybercrime, concerning the criminalisation of acts of a rasist and xenophobic nature commited through computer systems, http://conventions.coe.int.

[36] Council of Europe Convention on the Protection of Children against sexual exploitation and sexual abuse, http://conventions.coe.int.

[37] The Standford Draft International Convention to Enhance Security from Cyber Crime and Terrorism; http://fsi.standford.edu/publications/proposal_for_an_international_convention_on_cyber….

vzhledem k jejich velké rozmanitosti a proměnlivosti. Objevil se i názor, že USA jako nejsilnější a kybernetickými útoky nejzranitelnější země by si měly proto vytvořit „svůj vlastní právní rámec" pro potírání kybernetických útoků.[38]

Mezinárodní spoluprací v boji proti kybernetickému zločinu se zabýval např. XII. Kongres OSN o prevenci zločinu a trestní spravedlnosti, který se konal v Brazílii v srpnu 2010. Sekretariát Úřadu OSN pro tento kongres připravil materiál vyzývající „k přijetí globální úmluvy proti kybernetickému zločinu". Myšlenka získala silnou podporu v oblasti Asijsko-tichomořské ekonomické spolupráce, v EU, v Organizaci Amerických států a např. i v Interpolu. Kritická k návrhu byla např. Mezinárodní telekomunikační unie, váhavý postoj projevily nakonec např. Rusko a Brazílie nebo Čína. Rozdílné názory na standardy spolupráce komplikují uzavření globální konvence o kybernetických zločinech. Zájem o problematiku kybernetických zločinů však neutuchá. V květnu 2013 se např. v San Franciscu konala mezinárodní konference o kybernetických zločinech.[39]

3. KYBERNETICKÉ ÚTOKY A PRÁVO OZBROJENÝCH KONFLIKTŮ

Kybernetické operace použilo např. NATO v ozbrojené intervenci v Jugoslávii v roce 1999. Stejně tak byly porušeny nebo zničeny kybernetické sítě a telekomunikace v ozbrojené intervenci vedené USA proti Iráku v roce 2003. V dubnu 2007 došlo na protest proti přemístění sovětského pomníku z centra Tallinnu na předměstí k útokům DDOS na webové stránky estonské vlády, které trvaly déle než měsíc. Kratší útoky směřovaly proti bankám a sdělovacím prostředkům. Někteří oficiální estonští představitelé včetně ministra obrany hovořili o ohrožení národní bezpečnosti a „kybernetické válce". Estonsko obvinilo z útoků Rusko, které však svou angažovanost rozhodně popřelo. Přes spolupráci Estonska s počítačovými experty USA, Izraele a EU se nepodařilo bezpečně zjistit, kde mají tyto útoky svůj původ. Mezi estonskými představiteli se však objevily nesprávné názory, že kybernetické útoky již aktivovaly čl. 5 Severoatlantické smlouvy, zavazující NATO odpovědět na útok proti členovi aliance podle práva na kolektivní sebeobranu v souladu s čl. 51 Charty OSN. NATO na výzvu Estonska reagovalo vytvořením internetového obranného zařízení, které se v angličtině nazývá *Cooperative Cyber Defense Centre of Excellence* (CCDCOE).[40]

K použití kybernetického útoku v průběhu ozbrojeného konfliktu došlo zřejmě poprvé v roce 2008 v Jižní Osetii. Dne 7. srpna gruzínské jednotky zaútočily na ruské vojáky, kteří byli součástí mírových sil vytvořených na základě smlouvy mezi Gruzií a Ruskem z roku 1991. Více než tucet ruských vojáků bylo přitom zabito a mnoho dalších bylo zraněno. Rusko odpovědělo silným protiútokem a ozbrojený konflikt trval pouze několik dnů. Gruzie obvinila Rusko z útoku DDOS na webové stránky uživatelů v Gruzii, včetně

[38] http://www.stlr.org/2010/03/a-global-convention-on-cybercrime; viz k tomu např. Waxman M. C. Cyber Attacks and the Use of Force: Back to the Future of Article 2(4), The Yale Yearbook of International Law. 2011, N. 2, s. 425; též electronic copy available at http: //ssm.com/abstrakt=1674565. „…it will be difficult to achieve international agreement on legal interpretation and to enforce it with respect to cyber-attack", s. 425; Goldsmith, Cybersecurity Treaties: Sceptical View, viz http://mediahoover.org/sites/default/files/documents/.

[39] http://stegano.net/WCC2013, International workshop of cybercrime.

[40] NATO Cooperative Cyber Defence Centre of Excellence, http://ccdcoe.org/cycon/532.html nebo www.ccdcoe.org/278.html.

svých vládních orgánů, sdělovacích prostředků i komerční sféry. Ozbrojené ruské jednotky pronikly v odvetě hlouběji do vnitrozemí Gruzie. Metoda útoků DDOS s použitím „*malware*" (škodlivý software), infikující velký počet počítačů a vytvářející „*bootnets*" byla využita v útocích jak proti Estonsku v dubnu a květnu 2007 tak i proti Gruzii v srpnu 2008.

Kybernetickým útokům se státy brání na národní i mezinárodní úrovni. Z hlediska mezinárodního práva a suverenity států internet nezná a nerozlišuje státní hranice. Běžně se dnes setkáváme s pojmem „kybernetická válka" nebo „kybernetické vedení války". Státy dokonce vytvářejí nebo již vytvořily zvláštní organizační složky, zabývající se kybernetickými útoky, které působí v rámci ministerstev obrany, vnitra nebo jako speciální instituce. USA 21. 5. 2010 zřídily při Ministerstvu obrany „Kybernetické velení" (U.S. Cyber Command – USCYBERCOM), jehož prvním náčelníkem se stal čtyřhvězdičkový generál Keith B. Alexander. Sídlem USCYBERCOM je Fort Meade v Marylandu.[41] I další státy vytvářejí útvary určené k obraně proti eskalující hrozbě kybernetických útoků. Velká Británie vytvořila v září 2009 Středisko kybernetickobezpečnostních operací (Cyber Security Operations Centre) v rámci Vládního komunikačního ústředí (GCFQ). Také Francie založila v červenci 2009 svou Agenturu pro síťovou a informační bezpečnost. V Německu mají Cyber-Abwehrzentrum. V Číně podle některých informací existují dvě oddělení generálního štábu a řada útvarů se zabývá kybernetickou obranou a kybernetickou špionáží. V Rusku jsou otázky kybernetické bezpečnosti svěřeny jak Ministerstvu obrany, tak Federální bezpečnostní službě.[42]

Existuje podezření, že Hamás nebo Hizballáh atakují webové stránky v Izraeli. Zmiňuje se např. využití kybernetických útoků v izraelsko-libanonském konfliktu v roce 2006. Jsou také popsány útoky asi 3000 čínských hackerů v roce 1998 na webové stránky indonéské vlády jako výraz protestů proti postupu indonéské vlády vůči čínskému obyvatelstvu. V letech 2009–2010 počítačový vir nazývaný Stuxnet nebo také Stutznet napadl počítače v Íránu a jejich prostřednictvím íránský jaderný program. Íránský jaderný program měl „Stuxnet" opozdit až o několik let. Zasáhl však bohužel i 40 procent počítačů mimo Írán, a sice v Indii, Indonésii a Rusku. Byl zaměřen na manipulaci, respektive zničení určitého průmyslového procesu v oblasti jaderné energie. M. O'Connel spatřuje ve spuštění Stuxnetu Spojenými státy jejich ochotu porušit normy mezinárodního práva v kybernetickém prostoru.[43]

Kontroverzní termín „kybernetická válka" použili zřejmě poprvé dva pracovníci RAND Corporation John Arquilla a David Ronfeld v článku *Cyberwar is coming* v časopise Comparative Strategy v roce 2003. V literatuře se hovoří nejen o právním statusu „kybernetického válčení" (*cyber warfare*), nýbrž se používá i termín „kybernetická agrese" (*cyber aggression*) nebo „kybernetický válečný zločin".[44] V budoucnu nelze vyloučit, že k takovým zločinům může dojít (*cyber war crimes*).[45]

---

41 *British Encyclopaedia*, op. cit. 15, s. 183.

42 Ibid.

43 Srov.: „if the USA has released the Stuxnet virus, then the Word already has an example of willingness to violate international law in cyberspace". O'CONNEL, M. E. Cyber Security without Cyber War. *Journal of Conflicts and Security Law*, No 2, Oxford University Press, s. 199.

44 Článek „Cyberwar is Coming!" napsali vědečtí pracovníci z Rand Corporation pro časopis Comparative strategy v roce 1993, viz *Encyclopaedia Britanica*, 2011, Book of the Year, Chicago, London, s. 183.

45 GILMORE, S. A. *All Tomorrow's Massacres: Toward a Cybersecurity Framework for Mass Atrocity Crimes*, s. 33.

Kooperativní kyberneticko-obranné středisko NATO v Tallinnu (Cooperative Cyber Defence Centre of Excelence – NATOCCDCOE) každoročně organizuje mezinárodní konferenci věnovanou kybernetickým útokům. Poslední, pátá konference se uskutečnila v estonském Tallinnu v červnu 2013. Tyto konference se zaměřují na technické a právní implikace využívání automatických metod k odstranění kybernetických konfliktů. Na programu bývají dva okruhy problémů. Jeden je věnován strategickým a druhý technickým otázkám. Oba okruhy ovšem zahrnují i právní aspekty. Předmětem zkoumání jsou rozmanité otázky. Od definování kybernetického konfliktu na zemi, ve vzduchu, kosmickém prostoru, na moři i pod vodou, kybernetických zbraní, terminologie atp., až po taktické, operační a strategické postupy v kybernetickém prostoru při kybernetických útocích. Paleta projednávaných problémů tak např. zahrnuje vymezení kybernetického útoku jako nástroje politiky, dále pak ekonomické, vojenské a ideologické aspekty kybernetických útoků, problematiku kybernetických zločinů, různé aktéry kybernetických útoků (armáda, zpravodajské služby, obchodní činitelé, žoldnéři, teroristé, zločinci, hackeři), otázky kybernetických protiútoků, rozšíření kybernetických útoků za rámec kybernetické domény, včetně konvenčního vedení války, ověřování kybernetických útoků, odhalování kybernetických hrozeb atp.[46]

Válečné právo vznikalo v době kdy internet ani počítače neexistovaly. Přesto se v současnosti hovoří i ve smyslu válečného práva či práva ozbrojených konfliktů o „kybernetickém válčení“ nebo o „kybernetickém vedení války“ (*cyberwarfare*), aniž by byl uspokojivě vyřešen samotný obsah tohoto pojmu. Výzkumné středisko Kongresu USA např. vymezilo kybernetické vedení války celkem jednoduše jako „válčení v kybernetickém prostoru“, které „může zahrnovat ochranu informací a počítačových sítí, odrážení informačních útoků, jakož i narušování schopnosti protivníka učinit totéž“.[47] Pojem „kybernetického válčení“ a „kybernetické agrese“ se staly součástí obsahu různých kybernetických slovníků a odborných publikací, přesto nejsou ani tyto pojmy vymezovány jednotně. Stejně tak není jednotný názor, zda obrana proti „kybernetickým útokům“ má být vedena trestněprávními prostředky nebo prostředky válečného práva. Žádná komplexní mezinárodní smlouva, která by sankcionovala nelegální kybernetické útoky, neexistuje. Podle některých autorů musí proto státy jednat podle právní analogie. Většinou se navrhují dvě možnosti: buď přirovnat kybernetické útoky podle závažnosti k tradičním ozbrojeným útokům, nebo je považovat za trestnou činnost a jednat podle trestního práva.[48] Samotné vymezení kybernetického útoku označil jeden z autorů za „hádanku pro právníky“.[49] Podle většinového vymezení kybernetického vedení války se jedná o politicky, ekonomicky, vojensky i ideologicky motivované jednání rozbíjející internetový systém (*hacking*) jednoho nebo i více států, většinou s cílem ochromit národní hospodářství a obranyschopnost země nebo i špionáže. R. A. Clark knize *Cyber War* definuje kybernetické válčení jako činy jednoho státu k proniknutí do počítačů nebo sítí jiného státu s cílem

[46] 5th International Conference on Cyber Conflict 2013, 4–7 June Tallin, Estonie, www. Cedre.org.278.html.
[47] HILDRETH, Steven A. *Cyberwarfare, Congressional Research Service,* 16 (June 19, 2001).
[48] CARR, J. *Inside Cyber War*, kapitola 4.6. Analyzing Cyber Atacks Under Jus Ad Bellum, s. 176, viz též http://mysafaribooksonline.com/book/networking/security/9781449377229/the_law_of_war, s. 2.
[49] Srov. „Cyber attacks represent a conundrum for legal scholars…“ nebo „whether cyber attacks can qualify as armed attack and which cyber attacks should be considered armed attacks are left as open questions in international law“, ibid. s. 2.

způsobit škodu nebo nefunkčnost jeho počítačových sítí.[50] John Sheldon uvádí, že kybernetické vedení války je třeba odlišovat od kybernetických teroristických útoků, kybernetické špionáže nebo kybernetických zločinů.[51]

Kybernetické vedení války (*Cyber warfare*) je charakterizováno jako „válka vedená v kybernetickém prostoru kybernetickými prostředky a metodami". Kybernetický prostor je vymezován jako „globálně vzájemně propojená síť digitálních informačních a komunikačních infrastruktur, včetně internetu, telekomunikačních sítí, počítačových sítí a informací v nich obsažených".[52] N. Melzer, v souladu s koncepcí „U.S. Departement of Defence", rozlišuje neprávní pojem „kybernetická operace" (*cyber operation*) od mezinárodněprávních pojmů jako jsou např. „síla", „ozbrojený útok" nebo „útok". Kybernetické operace pak dělí na „počítačový síťový útok" (*computer network attack*), „počítačovou síťovou exploataci" (*computer network exploatation*) a „počítačovou síťovou obranu" (*computer network defence*). Útok na počítačové sítě (CNA) zahrnuje všechny kybernetické operace směřující k „poškození, popření, degradování nebo zničení informací obsažených v počítačích a počítačových sítích, nebo v počítačích a sítích samotných", exploatace počítačové sítě (CNE) spočívá v „umožnění operací a zpravodajského získávání a shromažďování dat z cílového počítače nebo automatizovaných informačních systémů protivníka". Konečně obrana počítačové sítě (CND) zahrnuje „akce na ochranu, monitorování, analyzování, odhalování a reakci na neoprávněnou činnost uvnitř informačních systémů a počítačových sítí" nebo ve zkratce obranu CNA a CNE pomocí rozvědné činnosti, kontrarozvědné činnosti, vynucením práva a vojenskými možnostmi.[53] Týž autor se zabývá též otázkou, zda válčící strana může legálně používat telekomunikační infrastrukturu neutrálních států pro účely kybernetických útoků a také odpovědností „neutrálních" států za nestátní válčící aktéry, provádějící útoky z jeho nebo přes jeho území nebo infrastrukturu. „Kybernetické válčení" nelze podle jeho názoru směšovat s „kybernetickou kriminalitou" nebo „kybernetickým terorismem", na které se mezinárodní humanitární právo nevztahuje.[54] Jistě je pravda, že na většinu kybernetických operací nebo útoků nelze aplikovat právo ozbrojených útoků, nicméně kybernetický útok stejně jako kybernetický terorismus může představovat mezinárodní zločin a kybernetický terorismus může být zřejmě i ozbrojeným útokem.

Sbor náčelníků štábů USA rozlišuje pět různých metod „kybernetických informačních operací": 1) elektronické válčení; 2) operace prostřednictvím počítačových sítí, včetně útoků na počítačové sítě; 3) psychologické operace; 4) vojenský podvod a 5) operační bezpečnost. Válčení prostřednictvím počítačových sítí jako součást širšího vedení informační války (*information warfare*) zahrnuje použití operací počítačových sítí (CNO) s úmyslem zabránit protivníkovi v účinném užívání počítačů jako informačních systé-

[50] CLARK, R. A. – KNAKE, R. A., op. cit. 1, s. 6.
[51] Op. cit. 18, s. 183.
[52] MELZER, N. Cyber warfare and International Law, *UNIDIR Resources*, 2011, s. 4. Jiné definice s podobným obsahem lze nalézt v „*The White House, Cyberspace Policy Review*" z 16. 5. 2011 nebo v „*The National Military Strategy for Cyberspace Operations of U.S. Departement of Defense*" (2006) či v „*U.S. Joint Chiefs of Staff, Departement of Defense Dictionary of Military and Associated Terms*" (2001).
[53] MELZER, N., op. cit. 52, s. 5; viz též *US Departement of Defence, The National Military Strategy for Cyberspace Operations*, 2006.
[54] Ibid.; s. 3–4.

mů a sítí, a to při současném využití vlastních počítačů, informačních systémů a sítí. Tyto operace pak zahrnují útok pomocí počítačové sítě (CNE) a obranu počítačových sítí.[55] R. A. Clark jako bezpečnostní expert americké vlády definoval kybernetické válčení široce jako „politicky motivované útoky (*hacking*) k provedení sabotáže a špionáže". Podle jeho názoru se jedná o formu informačního vedení války, které se někdy považuje za „analogické válčení konvenčními zbraněmi". Zároveň však připouštěl, že tato analogie je kontroverzní jak z důvodu její nepřesnosti tak i politických motivací. Kybernetickou válku charakterizoval jako „akce jednoho státu k proniknutí do počítačů nebo sítí za účelem způsobení škody nebo jejich nefunkčnosti".[56] Bývalý ředitel CIA a poradce Rady národní bezpečnosti USA M. Hayden definoval kybernetickou válku jako „záměrný pokus zneschopnit nebo zničit počítačové sítě jiných zemí".[57]

V mezinárodním pojmu se setkáváme s pojmy „ozbrojený útok" (zejména v rámci *ius ad bellum*) a „útok" (*ius in bello*), které mají různý význam i právní důsledky. Ve *Slovníku vojenských pojmů* vydaném Ministerstvem obrany USA je definován „počítačový síťový útok" (CNA) jako „akce podniknuté pomocí počítačových sítí k narušení, popření, degradování nebo zničení informací obsažených v počítacích a počítačových sítích nebo počítačích a sítích samotných".[58] M. N. Schmitt hovoří o „kybernetickém ozbrojeném útoku" podle *ius ad bellum* a „kybernetickém útoku" podle *ius in bello*.[59] Právo ozbrojených konfliktů lze aplikovat jen na malou část kybernetických útoků. Je však výjimečně obtížné dovodit, které počítačové útoky mají skutečně povahu ozbrojeného útoku, připouštějící možnost ozbrojené intervence na základě zmocnění RB. Zdá se být zřejmé, že základní zásady válečného práva jako jsou vojenská nutnost, proporcionalita a humanita, lze jen obtížně aplikovat i na kybernetické útoky. Testem, zda kybernetický útok přeroste do ozbrojeného útoku, je způsobená fyzická destrukce, nazývaná občas „kinetickým efektem", který je srovnatelný s účinky útoku konvenčními zbraněmi. Existují návrhy na revizi práva ozbrojených konfliktů s cílem dosáhnout konsensu o tom, kdy kybernetický útok je ozbrojeným útokem nebo jiným použitím síly.[60] Podle některých názorů lze určité kybernetické útoky již podřadit pod extenzivní interpretaci článku 2 odst. 4.[61]

NATO v *Common Approach to Cyber Defence* v dubnu 2008 uvedlo, že kybernetický útok vyvolává povinnosti členských států podle čl. 4 Severoatlantické smlouvy.[62] Článek

[55] Viz *U.S. Department of Defense. Department of Defense Strategy for Operating in Cyberspace* 2, July 2011.

[56] Srov. „…actions by a nation-state to penetrate another nation's computers on networks for the purposes of causing damage or disruption", Clark, A. R. – Knake, R. K., op. cit. 1, s. 6.

[57] Srov. …deliberate attempt to disable or destroy another country's computer networks, http://www.npr.org/templates/story.php?story/d=130023318.

[58] U.S. Departement od Defense. *Dictionary of Military and Associated Terms*. www.dtc.mil/doctrineded_dictionary.

[59] SCHMITT, M. N. „Attack" as a Term of Art in International Law: The Cyber Operations Context. In: C. Czosseck – R. Ottis – K. Ziolkowski (eds). *4th International Conference on Cyber Conflict*. 2012 NATO CCS Publications Talin, 2012, s. 286–289.

[60] …there is a growing need for states to reach a consensus as to when a cyber – attack constitutes an armed attack or use of force, viz např. HATHAWAY, O. A. et al., op. cit. 16, s. 840.

[61] Srov. též: „Any computer network attack that internationally causes any destructive effect within the sovereign territory of another state in a unlawful use of force within the meaning of Article 2(4) that may produce the effect on an armed attack prompting the right of self-defense", viz SHARP, W. G. Cyberspace and the Use of Force, 1999, s. 140.

[62] Viz *NATO Agrees on Common Approach to Cyber Defense 2008*, op. cit. 11, http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377.

se aktivuje v případě, že je ohrožena územní celistvost, politická nezávislost nebo bezpečnost některé ze smluvní strany organizace. Podle strategie NATO mají členské státy v případě kybernetického útoku „konzultovat" kybernetickou obranu podle čl. 4 smlouvy. Kybernetický útok však podle této strategie ještě neaktivuje čl. 5 Severoatlantické smlouvy o vzájemné pomoci. NATO v listopadu 2011 začalo připravovat *Cyber Warfare International Law Manual*, který zahrnuje otázky týkající se použití ozbrojené síly, mezinárodního humanitárního práva a související problémy suverenity, odpovědnosti států a neutrality.[63] Rovněž *White House Cyberspace Strategy* předpokládá, že kybernetické útoky mohou dosáhnout úrovně ozbrojeného útoku a tím vyvolat právo na sebeobranu podle čl. 51 Charty. USA v této strategii jasně deklarovaly, že na nepřátelské akce v kybernetickém prostoru, budou reagovat, jako na všechny jiné hrozby. Zmínily v této souvislosti právo na sebeobranu a plnění vojenských závazků.[64] Je zřejmé, že čl. 2 odst. 4 Charty zakazuje i použití síly a hrozby silou, které ještě nedosahují intenzity ozbrojeného útoku a nevyvolávají tak právo na sebeobranu podle čl. 51 Charty OSN.

Určení, zda lze kybernetický útok považovat i za ozbrojený útok závisí podle M. Schmitta na šesti faktorech, jimiž jsou: 1) závažnost, typ a rozsah škody; 2) bezprostřednost s jakou se újma projeví po útoku; 3) přímost, důsledky, které se projeví na vzniku újmy; 4) agresivita, s níž útok pronikne na území státu oběti; 5) stupeň měřitelnosti, jíž může být újma kvalifikována a kvantifikována; 6) presumptivní legitimita, která předpokládá, že kybernetický útok tvořící ozbrojený útok je spíše výjimkou než pravidlem.[65] Vyskytly se i názory (*the instrument-based approach*), podle nichž je ozbrojeným útokem každý kybernetický útok, který je veden proti důležitému počítačovému systému a ohrožuje tím národní infrastrukturu. V tomto pojetí pak kybernetický útok poskytuje napadenému právo na sebeobranu s použitím ozbrojené síly.[66]

Představitelé ministerstva obrany USA a Kybernetického velení jako zvláštního oddílu Strategického velení, které je posledním z devíti bojových útvarů Spojeného systému velení USA,[67] zdůrazňují připravenost armády odpovědět na nepřátelské činy v kybernetickém prostoru stejně jako na nepřátelské činy na zemi, ve vzduchu a na moři.[68] NATO má otázky kybernetické bezpečnosti zařazeny ve svém programu činnosti od konference

63 http://infosecisland.com/blogview/1871-NATO-Drafting-Cyber-Warfare-International… 29. 5. 2013.

64 International Strategy for Cyberspace, Prosperity, Security and Openess in a Networked World, White House, May 2011, s. 10, 14, viz http://www.white-house.gov/sites/default/files/rssviewer/international/strategy/for/cyberspace.pdf, Srov.: „When warranted the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners"…. „We will exhaust all options before military force whenever we can; will carefully weight the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible".

65 SCHMITT, M. N., op. cit. 31, s. 914–5.

66 SHARP, W. G., op. cit. 61, s. 140.

67 *US Department of Defence Cyber Command Fact Sheet*, 21. May 2010, http://www.stratcom.mil/facts-sheets/Cyber_Command//.

68 Just as our military is prepared to respond to hostile action land, air and sea, we must be prepared to respond to hostile act in cyberspace. Accordingly, the United States reserves the right, under the laws of armed conflict, to respond to serious cyber – attack, with a proportional and justified military response, at the time and place of its choosing. LYNN, W. Former Deputy Secretary of Defence, 2011, <http://www.pentagonchannel.milonestorypopup.aspx?pid=FttPuXny5i7D8p1hCOrgnXrveie.DVeMWM; viz též Lynn, W. J. Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs, Sept./Oct. 2010, s. 97–101.

v Praze v roce 2002. Vyvinulo a dále vyvíjí technologie a zařízení kybernetické obrany s cílem zabránit, odhalit a napravit důsledky kybernetických útoků, jakož i koordinovat národní kybernetické obranné systémy.[69] V roce 2008 v Estonsku vytvořené Středisko kybernetické obrany (CCDCOE) se zabývá výzkumem a přípravou na „kybernetické válčení".[70] V rámci organizační struktury NATO působí i další útvary zabývající se kybernetickou obranou. Jsou to orgán pro řízení kybernetické obrany (Cyber Defence Management Authority – CDMA) nebo útvar nazývaný „Způsobilost reagovat na počítačové incidenty" (The NATO Computer Incident Response Capability – NCIRC). První útvar má odpovědnost za koordinaci kybernetické obrany aliance a druhý řeší a informuje o kybernetických incidentech uživatele.[71] Strategie NATO vychází z předpokladu, že jednotlivé členské země nejsou schopny samostatně reagovat na všechny kybernetické hrozby. Strategie NATO z června 2011 počítá i s intenzivní spoluprací se soukromým sektorem.[72] Kybernetické vedení války je v Kongresu USA charakterizováno jako „válčení v kybernetickém prostoru".[73] Společnou kybernetickou bezpečnostní strategii prosazuje např. na regionální úrovni Organizace amerických států.[74] Problematikou kybernetických útoků a kybernetického vedení války se zabývá např. i Mezinárodní výbor Červeného kříže v Ženevě (ICRC). Experti i zde si kladou otázky o aplikovatelnosti mezinárodního humanitárního práva na kybernetický útok a jeho vztahu k definici ozbrojeného útoku.[75] Mezinárodní výbor Červeného kříže (ICRC) zastává jasné stanovisko, že válečné právo klade svá omezení i na kybernetické útoky a oceňuje Manuál NATO z Tallinnu, který potvrzuje, že mezinárodní humanitární právo (válečné právo) se vztahuje i na kybernetické válčení. Státy by měly být extrémně obezřetné při uchýlení se ke kybernetickým útokům, které by měly směřovat proti vojenským objektům a nikoli proti civilistům a civilní infrastruktuře.[76] V blízké budoucnosti se předpokládá existence kybernetických zbraní (*cyber weapons*). Objevil se již i názor, který v kybernetickém válčení spatřuje u nejzávažnějších kybernetických útoků dokonce analogii s jadernou válkou a s účinky jaderných zbraní. Uzavření smlouvy, která by zakázala kybernetické zbraně je podle tohoto názoru nesmírně obtížné, neboť počítačové kódy představující „informační válku" (*information warfare*) jsou často nerozlišitelné od nevinné žádosti o informaci.[77] Problematikou kybernetického válčení a mezinárodním právem se zabývají i pracovníci

[69] Strategic Concept for the Defense and Security of Members of the North Atlantic Treaty Organisation, 19 Nov. 2010, http://www.nato.int/lisbon2010/strategicconcept/-2010-eng.pdf, para 19.

[70] http://www.spacewar.compreport/NATOlaunches_cyber_defence_centre_in_Estonia_999.html>.

[71] Viz http://www.ndc.nato.int/research/series.php?code=1>, s. 8.

[72] Op. cit. 65.

[73] Srov. „Warfare waged in cyberspace", zahrnující „defending information and computer networks, deferring information attacks, as well as denying an adversary's ability to do the same. It can include offensive informations mounted against an adversary, or even dominating information on the battlefield"; Hildreth, S. A., op. cit. 44.

[74] Organization of American States, A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, viz http://www.oas.orgwww/vga/english/docs/approved/documents/adoption_strategy_combathreats_cybersecurity.htm.

[75] www.irc.org/eng/war-and-law/conduct-hostilities/information-warfare/index.

[76] ICRC, GISEL, L. *Legal adviser, The law of war imposes limits on cyber attacks too*; http://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm.

[77] SCHACKELFORD, S. J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeler Journal of International Law*, 2009, Vol. 27, issue 1, s. 216–217.

UNIDIR. N. Melzer, který je bývalým právním poradcem ICRC a jedním z expertů, kteří připravovali tallinnský manuál o mezinárodním právu aplikovatelný na kybernetický konflikt, rozlišuje kybernetické operace, které se mohou rovnat a) mezinárodně protiprávní hrozbě nebo použití „síly", b) „ozbrojenému útoku" ospravedlňujícímu uchýlení se k nezbytnému a proporcionálnímu použití síly v sebeobraně, nebo c) „hrozbě mezinárodnímu míru a bezpečnosti" nebo „porušení míru" opravňujícím k intervenci RB.[78] Proti názoru, že kybernetický útok může vyvolat tradiční právo sebeobrany, se vyslovila např. Čína a navrhla vypracování nových mezinárodních norem k lepšímu pochopení kybernetických hrozeb, včetně zneužití internetu k destabilizaci režimu. Rusko se vyslovovalo pro novou mezinárodní dohodu, která by v mezinárodním právu vyplnila „mezery" týkající se kybernetických zbraní.[79] Problematika kybernetických útoků je v odborné literatuře zkoumána nejen z hlediska právního, nýbrž současně i z hlediska politického a strategického.

V politickém slovníku se někdy hovoří i o již existující kybernetické válce.[80] Jsou dokonce autoři a političtí činitelé, kteří zdůrazňují potřebu rozvíjet kybernetickou strategii podobným způsobem, jako USA uplatňovaly strategii studené války a hovoří proto o „kybernetické studené válce".[81] Podle jiných autorů je naopak chybou pojímat kybernetický prostor jako bojiště, neboť skutečnými světovými problémy jsou kybernetické zločiny a špionáž.[82] Kybernetické válčení, kybernetickou válku nelze směšovat např. s kybernetickou špionáží nebo terorismem, i když některé teroristické činy mohou být zároveň kybernetickými útoky. Ve své mezinárodní strategii v kybernetickém prostoru USA počítají s použitím ozbrojené síly jako reakcí na nepřátelské činy v kybernetickém prostoru namířené proti USA a spojencům na základě „přirozeného práva na sebeobranu".[83] Někteří autoři uvádějí, že pro regulaci kybernetických útoků lze využít normy mezinárodního válečného práva a počítají s použitím ozbrojené síly.[84] Podle jiných názorů nehraje při regulaci kybernetických konfliktů mezinárodní právo podstatnější

78 MELZER, N., op. cit. 52.

79 Viz tomu WAXMAN, op. cit., s. 115.

80 Srov. „ The United States is fighting a cyber-war today, and we are losing…", McConnel Mike, former director of NSA, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR20100225024; Mc Connel „To Win the Cyber-War, Look to the Cold War", Washington Post, February 28, 2010, s. 31.

81 SINGER, P. – SCHACHTMAN, N. *The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive*. Brookings Institution 2011, http://ww.brookings.edu/articles/2011/0815_cyber_security_singershachtman.aspx, 20 June 2012.

82 Srov. „As already indicated…the emphassis on cyber space as battle space is in tension with the international law goverming the use of force" and „the real Word problems are crime and espionage". O'CONNEL, M. E., op. cit. 43, s. 198, 200.

83 Srov. „When warranted the United States will respond to hostile act in cyberspace… All states poses an inherent right to self-defense… We reserve the right of use all necessary means-diplomatic, informational, military and economic – as appropriate and consistant with applicable international law, in order to defend our Nation, our allies, our partners and our interests." *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rssviewer/internationalstrategy_for_cyberspace.pdf.

84 SCHMITT, M. N., op. cit. 57, s. 885; DINSTEIN, Y., srov.: „The novelty of the weapon-any weapon-always baffles statesmen and lawyers, many of whom are perplexed by technological innovation… After a period of gestation, it usually dawns on…that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon…." In: Computer Network Attacks and Self-Defence. *International Law Studies*. 2002, s. 99, 114–115.

roli. Dochází také k extenzivní interpretaci mezinárodního práva ospravedlňující širší použití síly, než povoluje Charta.[85]

Náčelník US Cyber Command, generál poručík Keith Alexander v roce 2010 dokonce prohlásil, že „neexistuje mezinárodní konsensus o přesné definici použití síly v nebo mimo kybernetický prostor". Jednotlivé státy mohou, podle jeho názoru, spatřovat „rozdílný práh toho, co představuje použití síly". Prezident USA může proto podle jeho názoru rozhodnout, že kybernetická událost dosahuje prahu použití síly / ozbrojeného útoku, který je takového rozsahu, trvání nebo intenzity, že opravňuje USA k výkonu práva sebeobrany a/nebo zahájení nepřátelství jako přiměřené odvety (response).[86] Oficiální pozice USA je vyjádřena ve strategii pro kybernetický prostor, která uvádí, že „v souladu s Chartou OSN státy mají přirozené právo na sebeobranu, které může být iniciováno jistými útočnými činy v kybernetickém prostoru".[87] USA tuto svou pozici v interpretaci čl. 51 Charty prezentovaly i ve zvláštní Skupině expertů OSN, kterou zmínil ve své zprávě z 15. 7. 2011 generální tajemník OSN. Stanovisko USA uvádělo, že může být v konkrétní situaci obtížné dosáhnout definitivní právní závěr, zda škodlivá činnost v kybernetickém prostoru představuje ozbrojený útok implikující právo na sebeobranu, nicméně se v něm konstatovalo, že USA „nepovažují za nutné vytvářet nový právní rámec pro kybernetický prostor", neboť je dostačující reflektovat tyto nové výzvy v již existujícím rámci Charty OSN. Podle stanoviska USA „za určitých okolností může ničivá činnost v kybernetickém prostoru představovat ozbrojený útok".[88] V roce 2011 USA spolu s Austrálií oznámily rozšíření smlouvy o vzájemné obraně přímo i na kybernetický prostor.[89]

K postoji vlády USA na právní regulaci činnosti v kybernetickém prostoru se autoritativně vyjádřil právní poradce Státního departmentu USA Harold Hongju Koh. V podstatě oficiální právní stanovisko vlády USA prezentoval 18. září 2012 na Inter Agency Legal Conference.[90] Koh si v první části přednášky položil celkem deset otázek, na které následně odpověděl. První část přednášky nazval „Mezinárodní právo v kybernetickém prostoru. Co víme". Druhá část byla nazvána „Mezinárodní právo v kybernetickém prostoru: výzvy a nejistoty". Třetí část přednášky zmiňovala „Úlohu mezinárodního práva v rozumném silovém přístupu (*smart power approach*) ke kybernetickému prostoru" a obsahovala závěrečnou otázku, zda je mezinárodní humanitární právo jediným mezinárodním právem, které se na kybernetický prostor aplikuje. Právní názor H. Koha se

---

85 Ibid.

86 LIEUTENANT, General Keith Alexander, Nominee for Commander, United States Cyber Command…, http://www.armed-service.senate.gov/statement/2010/04%20April/Alexander%2004-15-10.pdf.

87 Srov. „…consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace". *The White House, International Strategy for Cyberspace: Prosperity, security and Opennes in a Networked World 2011*, s. 10.

88 Srov. „…such ambiguities and room for disagreement do not in our view suggest the need for a new legal framework specific to cyberspace" nebo „under some circumstances, a disruptive activity could constitute an armed attack". *Report of the U.N. Secretary-General, Replies to the Developments in the Field of Information and Telecommunications in the Context of International Security.* Doc. A/66/152, July 15, 2011, s. 18.

89 US-Australia Ministerial Consultations, Joint Statement on Cyberspace, Sept. 15, 2011, http://www.state_gov./z/pa/prs/ps/2011/09/172490.

90 KOH, H. Lays Out US Government Position on Cyberspace and International Law; KOH, H. H. International Law in Cyberspace, viz opiniojuris.org/2012/09/19/herold-koh-on-international-law-in-cyberspace; viz též State Department Legal Adviser Addresses International Law in Cyberspace, 107, *American Journal of International Law*. 2013, No. 1, s. 243–248.

nepochybně promítl i ve stanoviscích akademické obce, zejména v USA. Hlavní závěry první části jeho referátu lze shrnout takto: 1) Mezinárodní právo se vztahuje i na kybernetický prostor; 2) Kybernetický prostor není „bezprávní" (*law free*) zónou, kde každý může vykonávat nepřátelskou činnost bez pravidel nebo omezení; 3) Kybernetické aktivity mohou, za jistých okolností představovat použití síly ve smyslu čl. 2 (4) Charty OSN a mezinárodního obyčejového práva; 4) Právo státu na sebeobranu, uznané v čl. 51 Charty OSN, může být vyvoláno aktivitami počítačové sítě, které se rovnají ozbrojenému útoku nebo jeho bezprostředně hrozící hrozbě; 5) V kontextu kybernetického konfliktu se právo ozbrojeného konfliktu aplikuje na úpravu použití kybernetických nástrojů v probíhajících nepřátelstvích, stejně jako na použití jiných nástrojů. Principy nutnosti a proporcionality omezují použití síly v sebeobraně a budou upravovat i to, co může tvořit podle okolností legální reakci; 6) Zásada rozlišování obsažená v *ius in bello* se vztahuje i na útoky počítačové sítě podniknuté v kontextu ozbrojeného útoku (podle Koha jde o kybernetické aktivity rovnající se „ozbrojenému útoku" a „legitimní vojenské cíle"); 7) Zásada proporcionality v *ius in bello* se aplikuje i na útoky počítačové sítě (*computer network attacks*), které jsou podniknuty v souvislosti s ozbrojeným útokem; 8) Státy by měly z právního hlediska přezkoumat své zbraně, včetně těch, které mají kybernetickou způsobilost, zda jsou přirozeně nediskriminační, tj. zda jejich použití je v souladu se zásadou rozlišení a proporcionality; 9) Státy provádějící činnosti v kybernetickém prostoru musejí brát v úvahu suverenitu jiných států, i mimo souvislosti s ozbrojeným útokem; 10) Státy jsou právně odpovědné za jednání jimi zmocněných osob (*through proxy actors*), které jednají podle instrukcí státu nebo pod jeho kontrolou.

K nedořešeným problémům podle druhé části referátu Koha patří otázka „jak může režim použití síly brát v úvahu všechny možné druhy účinků, vyvolané státy pouhým kliknutím počítače?". Jeho odpověď připomněla, že USA potvrdily „aplikovatelnost" pravidel *ius ad bellum* i na použití síly v kybernetickém prostoru (*use of force in cyberspace*). Koh zmínil případy, kdy fyzické účinky nepřátelských kybernetických akcí jsou srovnatelné s účinky kinetických zbraní. Uvedl např., že bomba může zničit přehradu a vytopit civilní obyvatelstvo stejně jako použití závadného počítačového kódu ze vzdáleného počítače. Kromě toho zmínil i jiné typy kybernetických aktivit, které podle něho vyvolávají otázku, co se přesně míní pojmem „síla v kybernetickém prostoru". Obtížnost dosáhnout konsenzu o tom, „kdy a za jakých okolností nepřátelský kybernetický čin" představuje „ozbrojený útok", podle Koha ještě automaticky neznamená potřebu „zcela nového právního rámce specificky pro kybernetický prostor". Podpořil tak spíše skeptický postoj USA k uzavření univerzální mezinárodní úmluvy. Druhá jeho otázka se týkala „dvojitého užívání infrastruktury" (*dual of use infrastructure*) v kybernetickém prostoru. Zde Koh zdůraznil, že válečné právo požaduje, aby civilní infrastruktura nebyla využívána pro „imunizování" (*to immunize*) vojenských cílů před útokem, včetně kybernetické sféry či domény. Třetí nedotčenou otázkou je podle Koha „přičitatelnost" (*attribution*) činností v kybernetickém prostoru, což je i podle Koha více otázka technická a politická než právní. Jeho vyjádření ani nepředpokládá, že všechny odpovědi na vznikající otázky kybernetického prostoru jako nového a dynamicky se rozvíjejícího prostředí budou právní („*We cannot expect that all answers…we face will be legal ones*"). V třetí části referátu autor zdůraznil, že mezinárodní humanitární právo není jediné mezinárodní právo (*It is not only international law*), které se v kybernetickém prostoru aplikuje. Zmínil zde

normy z oblasti lidských práv, obecně otázky kybernetické bezpečnosti, kybernetických obchodů, kybernetických zločinů, „pirátství" v oblasti průmyslového vlastnictví atp. Závěrem referátu Koh zdůraznil, že respektování norem mezinárodního práva umožňuje americké vládě jednat v kybernetickém prostoru „více a více legitimně" způsobem, který plněji podporuje „národní zájmy USA".[91]

Ne všechny kybernetické útoky představují kybernetické válčení ve smyslu práva ozbrojených konfliktů. Pouze kybernetické útoky s účinky, které jsou srovnatelné s účinky konvenčního „ozbrojeného útoku", nebo které nastaly v souvislosti s ozbrojeným útokem, dosahují úrovně „kybernetického válčení".[92] Válka obvykle probíhá ve čtyřech oblastech – na zemi, na moři, ve vzduchu, v kosmickém prostoru a v poslední době se hovoří ještě o páté doméně – kybernetickém prostoru.[93] Podle ojedinělých názorů pouze ty kybernetické útoky, které zahrnují použití vojenských zbraní, mohou dosáhnout úrovně ozbrojeného útoku.[94] Není pochyb, že vzrůstá důraz na militarizaci otázek kybernetické bezpečnosti spolu s rozšiřující se interpretací práva použít ozbrojenou sílu podle čl. 2 odst. 4 Charty nebo práva na sebeobranu podle čl. 51 Charty, jakož i extenzivním výkladem norem mezinárodního obyčejového práva.

Mezi vojenskými a bezpečnostními experty a činiteli dochází občas ke skeptickému pohledu na úlohu mezinárodního práva při regulaci využívání kybernetického prostoru. Právník Steward Baker, který byl podtajemníkem na Ministerstvu vnitřní bezpečnosti USA pro otázky politiky a technologií za vlády prezidenta Bushe, odmítal uznat úlohu mezinárodního práva obecně a jeho význam při ochraně kybernetické bezpečnosti zvláště. V diskuzi sponzorované Americkou společností pro mezinárodní právo v roce 2012 např. uvedl: „Právníci napříč americkou vládou vznesli tak mnoho „show-stoping" právních otázek o kybernetické válce, že ponechali naše vojáky neschopnými bojovat nebo dokonce plánovat válku v kybernetickém prostoru".[95] Podobně se Baker vyjádřil i v roce 2011 v časopise *Foreign Policy*.[96] Pro jiné autory je naopak problémem vtěsnat problémy kybernetického útoku do norem mezinárodního práva o zákazu použití síly. Navrhují proto v případě kybernetických útoků aplikovat především zásady a normy mezinárodního práva, týkající se nevměšování, protiopatření (*countermeasures*) a ekonomických sankcí. Podle Mary E. O'Connel i v případě, že by některé kybernetické incidenty

[91] Srov. „Because compliance with international law in cyberspace is part and parcel of our broder smart power approach to international law as part of U.S. foreign policy.", ibid. s. 5.

[92] Srov. „But not all cyber-attacks are cyber-warfare. Only cyber-attacks with effects equivalent to those of a conventional „armed attack" or occuring within the context of armed conflicts, rise to the level of cyber-warfare….", viz HATHAWAY, O., op. cit. 16, s. 846.

[93] War in the Fifth Domain, The Economist July 1, 2010, viz http://www.economist.com/mode/16478792. Viz též Joint Chiefs of Staff, The National Military Strategy of the United States of America, 2004, http://www.strategicstudiesinstitute.army.mil/pdffiles/nms2004.pdf.

[94] Srov. „This approach treats a cyber-attack as an armed attack only if it uses military weapons" nebo „a cyber-attack alone will almost never constitute an armed attack for purposes of Article 51, because it lacks the physical characteristics traditionally associated with military coercion" – in other words because it generally does not use traditional military weapons, viz k tomu HATHAWAY, O. A., op. cit. 16, s. 844.

[95] BAKER, S. A. – DUNLAP, C. J. *What is the Role of Lawyers in Cyberwarfare?* viz http://www.abajournal.com/magazine/article/what/is/the/role/of/lawyers/in/cyberwarfare.

[96] BAKER, S. Denial of Service, Against Cyberwar with Arcane Rules and Regulations. *Foreign Policy*, 30 September 2011, k tomu viz O'Connel, M. E., op. cit. 43, s. 189, srov. http://www.foreignpolicy.com/articles/2011/0930/denial/of/service?codecomments=yes.

i odpovídaly svou povahou definici ozbrojeného útoku, reakce na takový útok s použitím síly by byla jen výjimečně legální a rozumná.[97] O'Connel dále uvádí, že reakce na kybernetický útok by měla klást důraz na právní normy a závazky v nevojenské sféře. Hovoří dokonce o tom, že v USA a v jiných státech, kde se uvažuje o reakcích na kybernetické problémy v konvenčních vojenských termínech, jsou proponenti tohoto myšlení sami chyceni do pasti „ideologie militarismu".[98]

Americký Kongres se od roku 2011 zabývá novou legislativou v otázkách kybernetické bezpečnosti. Diskutovalo se i o tom, kdo má mít hlavní odpovědnost, zda Ministerstvo pro vnitřní záležitosti (DHS) nebo Pentagon a Národní bezpečnostní agentura (NSA). Nakonec zřejmě zvítězila s podporou kyberneticko-bezpečnostního průmyslového komplexu tendence k „militarizaci" kybernetické bezpečnosti a převahu získalo Ministerstvo obrany USA. Není vyloučeno, že svět stojí na prahu nové dimenze válečných konfliktů s použitím „kybernetických zbraní", které mohou postupně i částečně nahradit „klasické" zbraňové systémy. Do budoucna je nutno počítat s tím, že kybernetické útoky mohou rozrušit nebo i zcela zničit veškerou infrastrukturu jednotlivých států, bez použití doposud známých zbraní. V žádném případě však nelze zapomínat, že internet je mezinárodním statkem, který si zaslouží mezinárodněprávní ochranu.[99]

4. POZNÁMKA K OTÁZKÁM ODPOVĚDNOSTI

S kybernetickými útoky úzce souvisí i otázka mezinárodněprávní odpovědnosti států za tyto činy. V klasickém mezinárodním právu stát neodpovídal za činy svých občanů jako soukromých osob. V soudobém mezinárodním právu jsou otázky přímé odpovědnosti států řešeny zejména v Návrhu článků o odpovědnosti států, který v podstatné míře reflektuje mezinárodní obyčejové právo. Stát, který se stal obětí takového útoku, má právo uchýlit se k „aktivní obraně" (*active defences*) a použít i elektronická protiopatření (*countermeasures*) s cílem vyřadit útočící počítačový systém z provozu a tím kybernetický útok zastavit. Kybernetická sebeobrana by měla směřovat pouze proti státu, který přímo kybernetický útok vyvolal, nebo jehož zástupci (agenti) takový útok způsobili. Vzhledem k anonymitě počítačové technologie i možnému zneužití počítačových systémů (*zombies*) v třetích zemích není snadné původce útoků určit. V soudobém mezinárodním právu může být odpovědnost státu též založena na „přičitatelnosti" (*imputed responsibility*) činů nestátních aktérů, spáchaných na území konkrétního státu. Tento druh odpovědnosti je přímo revoluční a v mezinárodním právu nový. Impuls byl dán teroristickými útoky z 11. září 2001. V rezoluci RB OSN č. 1368 z 12. 9. 2001 bylo uvedeno, že šlo o „hrozbu proti míru a bezpečnosti", která „legitimizovala" vojenskou akci

97 Srov. „Even if some cyber incidents could fit a solid definition of what constitutes an armed attack, responding to such an attack will rarely be lawful or prudent in the response is a use of force." O'CONNEL, M. E., op. cit., s. 43, s. 191.

98 Srov. „In the USA and other States where the thinking is in the conventional military terms respecting responses to cyber problems, the advocates of such thinking appear to be trapped by an ideology of militarism." Ibid., s. 190–1.

99 Viz KETTEMAN, M. C. Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühling. *Zeitschrift für öffentliches Recht und Völkerrecht.* 2012, Nr. 2, s. 469–482.

USA v Afghánistánu proti Tálibánu a al-Kajdě jako akt sebeobrany. MSD ještě v kauze Nikaragua v USA odmítl uznat odpovědnost USA za činy „kontras", i když USA v Nikaragui organizovaly, trénovaly, financovaly a zbraněmi vybavily rebely bojující proti vládě v Nikaragui. MSD vycházel z názoru, že stát (USA) nemůže být odpovědný za činy nestátních aktérů, pokud nemá účinnou kontrolu vojenských nebo paravojenských operací rebelů, během nichž došlo k tvrzeným porušením práva.[100] K určitému posunu došlo v rozhodnutí Mezinárodního trestního tribunálu pro bývalou Jugoslávii v r. 1999, který v kauze Tadic vyslovil názor, že stát může být odpovědný za akce ozbrojených skupin, jestliže tento stát koordinoval nebo pomáhal při plánování činnosti těchto skupin.[101] ICTY tedy již nevyžadoval, aby stát měl efektivní kontrolu nad nestátními aktéry a spokojil se s všeobecnou (*overall*) kontrolou pro přičitatelnost spáchaných činů. Návrh článků o odpovědnosti státu za protiprávní chování řeší otázky přičitatelnosti chování státu v kapitole II. Na náš problém se vztahuje zřejmě čl. 9: „Chování osob nebo skupiny osob bude považováno za čin státu podle mezinárodního práva, pokud osoba nebo skupina osob ve skutečnosti provádějí prvky vládní moci v nepřítomnosti nebo v důsledku opomenutí oficiálních orgánů a za takových okolností, které vyzývají k výkonu těchto prvků moci."[102] Lze tedy vyvodit, že stát má povinnost zabránit kybernetickým útokům pocházejícím z jeho území a nese právní odpovědnost za posouzení takové odpovědnosti. Nepochybně u „přičitatelnosti" odpovědnosti konkrétnímu státu může dojít i k omylu nebo i zneužití. V rámci objektivity rozhodování je proto pro „odpovědný stát" nutné uskutečnit smysluplné a podrobné vyšetřování kybernetického útoku; stíhat ty, kteří se na těchto útocích podíleli; spolupracovat se státem – obětí kybernetického útoku na vyšetřování a stíhání odpovědných osob.[103] Odpovědnost státu může vzniknout v důsledku jeho chování nebo opomenutí. Některé kybernetické útoky mohou přerůst „práh", který z útoku kybernetického činí „ozbrojený kybernetický útok" ohrožující nebo porušující mezinárodní mír a bezpečnost. Jiné kybernetické útoky mohou představovat běžnou počítačovou kriminalitu.[104] Právo ozbrojených konfliktů (*ius in bello*) předpokládá zřejmě, i pro kybernetické útoky, respektování principů vojenské nutnosti a proporcionality, rozlišování kombatantů a nekombatantů, ochranu civilistů a civilních objektů. Zakázáno je používání zbraní, které působí zbytečné utrpení nebo i smrt. Stát reagující na kybernetický útok legálním a legitimním výkonem práva sebeobrany může reagovat i použitím kinetických zbraní, které ovšem nemusí být vždy efektivní. Podle převažujícího názoru v literatuře určité kybernetické útoky lze považovat za „ozbrojený útok".[105]

---

100 ICJ Reports 1986, Case Concerning Military and Paramilitary Activities In and Against Nicaragua, bod 292, s. 136, srov. „Decides that the United States of America, by training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities in and against Nicaragua, has acted, against the Republic of Nicaragua, in breach of its obligation under customary international law not to intervene in the affairs of another State …."

101 Prosecutor v Tadic, Case No. IT-94-1-A, ICTY, July 15, 1999, s. 49.

102 MRÁZEK, J. *Dokumenty ke studiu mezinárodního práva.* Plzeň: Aleš Čeněk, 2005, s. 118, ILC, Draft Articles on Responsibility of States for International Wrongful Acts, 2001, http://www.ilsa.org/jessup/jessup06/basicmats2/DARS.pdf.

103 Viz např. GRAHAM, D. E. Cyber Threats and the Law of War. *Journal of National Security Law and Policy.* 2010, s. 100.

104 K běžné kriminalitě viz např. BUCKLAND, J. (ed.). *Combating Computer Crime, Prevention.* Detec-McGraw-Hill, 1992.

Problémy odpovědnosti související s činností v kybernetickém prostoru jsou mnohem širší a zaslouží si samostatnou studii, na kterou zde není dostatečný prostor. Nejedná se ovšem pouze o otázky mezinárodněprávní.

5. STRUČNÝ ZÁVĚR

Kybernetický prostor nemůže být předmětem přivlastnění žádného státu. Autor se domnívá, že přínosem by byla univerzální úmluva, která by řešila otázky využívání kybernetického prostoru a kybernetické bezpečnosti. Bohužel jsme svědky, že používané termíny nejsou jednotné a je jim často přiřazován i rozdílný obsah. Pojmy „kybernetický útok", „kybernetická operace", „kybernetický incident" nebo „kybernetický zločin" jsou často používány promiscue bez přílišného ohledu na to, co vlastně znamenají. Sjednocení základních pojmů by přispělo nepochybně k posílení mezinárodní spolupráce v této oblasti. Autor chtěl původně zkoumat především pojetí určitých „kybernetických útoků" ve smyslu použití síly (útoku) podle čl. 2 odst. 4 Charty a „ozbrojeného útoku" ve smyslu čl. 51 Charty OSN. Vzhledem k tomu, že doposud nebyla v naší literatuře věnována náležitá pozornost „kybernetickým operacím" a „kybernetickému prostoru" z pohledu mezinárodního práva, bylo snad vhodné se pro lepší orientaci alespoň zmínit i o těchto souvisejících otázkách. Nebylo možné se proto vyhnout i určité popisnosti některých problémů. Pokud jde o pojetí určitých kybernetických útoků ve smyslu práva ozbrojených útoků, může být jen jejich malá část regulována právem ozbrojených konfliktů, a to na základě analogie a aplikace obecných principů práva ozbrojených konfliktů. Technologický vývoj kybernetiky předstihl úpravu v mezinárodním právu a některé státy si zatím takovou obecnou úpravu z různých důvodů ani nepřejí. Nejširším používaným všezahrnujícím pojmem jsou zřejmě „kybernetické operace", následovány „kybernetickými útoky" a „kybernetickými incidenty". Měly by být rozlišovány např. „kybernetické útoky" a „kybernetické zločiny". Mnohdy se uvedené pojmy také překrývají. V oblasti práva ozbrojených konfliktů bude někdy obtížné odlišit „kybernetické vedení ozbrojeného konfliktu" a „kybernetický ozbrojený konflikt" (válku), neboť v současnosti si nelze žádný ozbrojený konflikt bez využití kybernetických prostředků ani představit. V podstatě každý ozbrojený konflikt (válka) je dnes svým způsobem elektronický.

Nejširším používaným pojmem je zřejmě pojem kybernetického zločinu, který se vztahuje především na nestátní aktéry. Je otázka, zda se počítačového zločinu může dopustit i státní orgán, který překročil své úřední povinnosti a nejednal již jako státní orgán. Stejně tak lze klást otázku, zda akce státního orgánu s politickým nebo bezpečnostním podtextem budou vždy „kybernetickým útokem". Nebo zda všechny kybernetické zločiny spáchané nestátním aktérem z politických nebo bezpečnostních důvodů budou rovněž „kybernetickým útokem".[106] Podle našeho názoru nikoli, neboť nemůže záležet

[105] It is possible to conclude that certain vyber attacts can be deemed armed attacks". GRAHAM, D. E., op. cit. 103, s. 101.

[106] Toto stanovisko zastává např. O. A. HATHAWAY, op. cit. 16, s. 864. Srov.: „A political or national security purpose distinguishes cyber-attack from simple cyber-crime. Any aggressive action taken by a state actor in the cyber-domain necessarily implicates national security and is therefore a cyber-attack (where the action satisfies all the other elements of the definition), whether or not it rises to the level of cyber-warfare. Cybercrime committed by a non-state actor for a political or national security purpose is a cyber-attack."

jen na politickém nebo jiném účelu. Jak bylo v článku ukázáno, existují široká i úzká vymezení „kybernetického útoku“ a rozlišení státních a nestátních aktérů, hraje důležitou roli v otázkách právní odpovědnosti za spáchané činy. U nestátních aktérů je pak důležitá otázka „přičitatelnosti“ jejich činů a odpovědnosti za ně odpovědnému státu.

Kybernetickými zločiny lze rozumět spáchání nezákonných činů prostřednictvím počítačů, počítačových sítí a hardwaru a předpokládá se, že pachateli běžných kybernetických zločinů jsou fyzické osoby nikoli státy. I státní orgán se však může dopustit zločinu podle mezinárodního práva a nést trestní odpovědnost.

Velká většina kybernetických zločinů nebude „kybernetickým útokem“ v úzkém slova smyslu, jak jsme ho v článku popsali. Stejně tak některé „kybernetické útoky“ nebudou představovat „zločiny“ a nepůjde ani o „kybernetické vedení války“. Kybernetické vedení války bude zahrnovat i „kybernetické útoky“. Kybernetické vedení války může ovšem vést ke „kybernetickým zločinům“ a to i zločinům mezinárodním, respektive podle mezinárodního práva.

Autor se také domnívá, a rostoucí konsensus to potvrzuje, že určité kybernetické útoky mohou představovat „ozbrojený útok“ nebo alespoň prosté použití ozbrojené síly.

Kybernetickou bezpečností se začala zabývat i naše Sněmovna a výsledkem by měl být příslušný zákon, který by měl stanovit pravidla spolupráce mezi soukromým sektorem a veřejnou správou při předcházení útokům na informační technologie. Předpokládá se, že bude přijata i směrnice k zajištění bezpečnosti sítí a informací v EU. V ČR má hlavní gesci při zpracování zákona a také odpovědnost za vyhlášení (rozhoduje ředitel) stavu kybernetického nebezpečí v případě ohrožení bezpečnosti informací velkého rozsahu v informačních systémech nebo sítích elektronických komunikací Národní bezpečnostní úřad (NBÚ). Ředitel NBÚ může v určitých případech požádat vládu o vyhlášení „nouzového stavu“. V roce 2011 vláda zřídila Národní centrum kybernetické bezpečnosti v rámci NBÚ. Součástí centra by mělo být do roku 2015 vládní koordinační místo pro okamžitou reakci na „počítačové incidenty“ (CERT).

Stať vznikla s podporou na dlouhodobý koncepční rozvoj výzkumné organizace Ústavu státu a práva AV ČR, v. v. i., RVO: 68378122.

JUDr. Josef Mrázek, DrSc.
Ústav státu a práva AV ČR, v. v. i.
Fakulta právnická Západočeské univerzity v Plzni

Josef Mrázek

Cyber Space and International Law

Abstract: *The number of different cyber operations including cyber attacks are rising. Cyber threats represents serious risks to both public and private sectors, endangering cyber security of individual states and international security as a whole. Cyber attacks consists of various actions desrupting, denying or destroying computers and computers networks. There is also a growing tendency for militarization of cyber security. NATO is developing policies and capacity armed at cyberwarfare as a new "battlefield". The USA established Cyber Command as a part of "National military strategy". Some cyber attacks may be equated to armed attack with following response under the law of armed conflicts. This study is dealing with cyber security, cyber attack and cyber crimes. The only existing international convention in this respect is the European Convention on Cybercrime. In the author's view any activity in cyber space must comply with the rules of international law. The crucial question of this study is when the cyber (computer) attack may constitute use of force (casus belli) which amounts to an armed attack implicating a right to self defense under Art 51 of the UN Charter. The reply is in some serious cases positive.*

Key words: *Cyber operations, cyber attack, cyber security, cyber crime, cyber warfare*