Aplikace mezinárodního práva v kybernetickém prostoru a regulace autonomních zbraňových systémů

Luděk Jiráček je spolupracovníkem Výzkumného centra AMO se zaměřením na bezpečnostní politiku a Severoatlantickou alianci. Email: ludek.jiracek@amo.cz.

Abstrakt

Stať se zabývá tvorbou a možnou aplikací současného mezinárodního práva při řešení konfliktů v kybernetickém prostoru. Určitá pozornost je věnovaná fenoménu umělé inteligence, která se stává jednou ze strategických investičních oblastí soukromých společností a zároveň jedním z možných budoucích pilířů obranného průmyslu pro posílení pozic národních vlád v mezinárodních vztazích či pro posílení pozic na samotných bojištích.

Abstract

This paper deals with the creation and possible applications of the contemporary international law in resolving conflicts in cyberspace. Some attention is devoted to the phenomenon of artificial intelligence, which is becoming one of the strategic investment areas for private companies and, at the same time, one of the possible future pillars of the defence industry to strengthen the position of national governments in international relations and/or to strengthen positions on the battlefields themselves.

Klíčová slova

Kybernetická bezpečnost; kybernetické útoky; umělá inteligence; mezinárodní právo; Organizace spojených národů; Severoatlantická aliance.

Keywords

Cyber security; Cyber attacks; Artificial intelligence; International law; United Nations, North Atlantic Treaty Organization.

Úvod

Vývoj informačních technologií a možnosti využití umělé inteligence (AI) ovlivňují nejen fungování veřejného a soukromého sektoru, včetně chování lidí, ale zároveň mohou změnit přístup v tvorbě mezinárodního práva. Mimoto moderní technologie přináší nové hrozby, na které jsou národní vlády a mezinárodní organizace nuceny reagovat. Současný mezinárodní právní řád však nemusí vždy odpovídat novým typům konfliktů a válkám mezi různorodými aktéry v nových operačních oblastech, což se v praxi například ukázalo během kybernetických útoků v Estonsku v roce 2007. Pokud však mezinárodní organizace nebudou schopny aktivně reagovat na možné útoky, může to vést až k jejich zániku a narušení relativního míru na globální úrovni.

Cílem tohoto policy paperu je objasnit základní a zásadní problémy při možné aplikaci mezinárodního práva v kybernetickém prostředí a samotné klasifikaci zásadních pojmů. Mezi hlavní výzkumnou oblast bude patřit i aplikace mezinárodního práva na možnou budoucí hrozbu v podobě zneužití AI v obranném průmyslu. Stať se bude věnovat také roli mezinárodních organizací bezpečnostního typu (organizace kolektivní obrany – NATO a organizace kolektivní bezpečnosti – OSN) při řešení novodobých hrozeb spojených s kybernetickými útoky a využití AI při ozbrojených operacích.

1 Teoretický rámec kybernetické bezpečnosti

Definice pojmů je zásadním elementem nejen pro porozumění dané problematiky, ale zejména pro tvorbu možných legislativních opatření na národní i mezinárodní úrovni. Zavedení jednotné a jasné definice pro kybernetickou bezpečnost a samotnou klasifikaci kybernetické útoků je však velmi problematické a komplikované.[1]

Konflikty jsou z historického hlediska zakotveny v lidské přirozenosti a jednotlivé technologie jsou využívány i k destruktivním účelům. V současné době mezi takovéto technologie patří počítače využívané pro vedení války, a to za pomocí politicky či strategicky motivovaných kybernetických útoků a protiútoků.[2] V angličtině je možné se setkat s termíny Cyber war či Cyber warfare. Tyto útoky a zároveň veškerá elektronická komunikace probíhají v kybernetickém prostoru (angl. Cyberspace), který je tvořen „*informačními systémy,*

[1] Michael Schmitt, "Classification of Cyber Conflict," *Journal of Conflict and Security Law*, 2012, 17 (2), http://jcsl.oxfordjournals.org/content/17/2/245.full#xref-fn-18-1 (accessed 10. 12. 2016).
[2] Petr Jirásek, Luděk Novák and Josef Požár, "Výkladový slovník kybernetické bezpečnosti," Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2013, https://www.govcert.cz/download/aktuality/container-nodeid-548/slovnikv231nbuwebcolor.pdf (accessed 10. 12. 2016), 58.

a službami a sítěmi elektronických komunikací.“[3] Cílem takovýchto útoků je poškodit IT infrastrukturu či získat informace. Ty mohou být i v podobě tzv. kyberterorismu (angl. Cyber terrorism), jejichž cílem je za pomocí kybernetických útoků vyvolat strach. Vývoj technologií tak posouvá konflikty z konvenční úrovně na kybernetickou úroveň.

Povaha takovýchto útoků bývá v praxi mezinárodní, nikoliv vnitrostátní. Díky své asymetrii, jsou státní i nestátní aktéři schopni destabilizovat jednotlivé země bez použití konvenčních sil, a to například prostřednictvím útoků vůči kritické infrastruktuře.[4] Ta představuje „*systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva*.“[5] Mezi klíčové systémy kritické infrastruktury lze zařadit energetický průmysl, zdravotnictví, telekomunikační a poštovní služby, obranný průmysl, dopravní infrastrukturu, finanční a bankovní sektor, chemický průmysl, apod.

Co se týče samotného termínu kybernetická bezpečnost, tu lze charakterizovat jako „*souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*.“[6] Pojetí kybernetické bezpečnosti může být však v každé zemi chápáno odlišně. Například pro Ruskou federaci je kybernetická bezpečnost pojímána jako hybridní koncept, tedy jako součást informační války kombinující vojenský i nevojenský řád v širším kontextu.[7]

K eliminaci hrozeb a snížení rizik slouží tzv. kybernetická obrana. Zásadní překážkou pro kybernetickou obranu je však velmi rychlý rozvoj informačních a komunikačních technologií, které lineárně ovlivňují nejen soukromý a veřejný sektor, ale zároveň civilní obyvatelstvo. Se zvyšující se závislostí na takovýchto systémech totiž rozvoj vede v ruku v ruce i ke zvýšení rizika možného zneužití.

2 Typologie kybernetických útoků

V uplynulých dekádách bylo možné zaznamenat nespočet kybernetických útoků. Ty lze definovat jako "*operace v kyberprostoru, ať už ofenzivní, nebo defenzivní, v jejímž důsledku je*

[3] Petr Jirásek, Luděk Novák and Josef Požár, ”Výkladový slovník,” 59.
[4] Luděk Jiráček, ”Cyber security threats: the case of the Czech Republic,” in *Poland, the Czech Republic and NATO in Fragile Security Contexts*, edited by Anna Visvizi and Tomasz Stępniewski, 2016, http://www.amo.cz/wp-content/uploads/2016/12/Poland-the-Czech-Republic-and-NATO-in-Fragile-Security-Contexts.pdf (accessed December 16, 2016), 64.
[5] Petr Jirásek, Luděk Novák and Josef Požár, ”Výkladový slovník,” 55.
[6] Ibid., 57.
[7] Miroslava Pavlíková, ”KYBERNETICKÝ BOJ MEZI RUSKEM A UKRAJINOU V RÁMCI UKRAJINSKÉHO KONFLIKTU,” *Obrana a strategie*, vol. 1, 2016, http://www.obranaastrategie.cz/cs/archiv/rocnik-2016/1-2016/clanky/kyberneticky-boj-mezi-ruskem-a-ukrajinou-v-ramci-ukrajinskeho-konfliktu.html#13 (accessed December 10, 2016).

důvodné očekávat způsobení zranění či smrti osobám, nebo poškození či zničení věcí."[8] Z globálního hlediska však nelze nalézt jednotnou shodu na tom, co lze považovat za kybernetický útok. Definice toho, proti čemu je nutné se bránit či co je nutné regulovat, je však zásadní. Na neexistující jednotnou definici v oblasti kybernetické bezpečnosti upozorňuje i NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).[9] Spojené státy například doposud ani veřejně nedeklarovaly, v jakém případě by reagovaly na kybernetický útok, respektive kdy by představoval akt válečného konfliktu.[10]

V roce 2008, před samotným konfliktem mezi Ruskou federací a Gruzií, proběhlo napadení gruzínských serverů hackery. V roce 2010 se uskutečnil útok na závod na obohacování uranu v Iránu, a to za pomocí červu STUXNET, který změnil frekvenci otáček několika stovek centrifug. Mezi další útoky v oblasti energetiky, které patří mezi útoky na kritickou infrastrukturu, lze zařadit kybernetický útok na servery společnosti Korea Hydro & Nuclear Power či výpadek elektrické energie na Ukrajině v prosinci roku 2015.[11] Součástí ruské anexe Krymu byly dle ředitele Národního bezpečnostního úřadu Dušana Navrátila i útoky cílené na komunikační infrastrukturu.[12] V roce 2009 proběhly masivní DDoS útoky na vládní webové stránky v Estonsku, které nastaly v návaznosti na demonstrace kvůli přesunutí sovětského památníku mimo oblast Tallinnu. Estonská vláda z útoku přímo obvinila Ruskou federaci. Na základě investigace se však došlo k závěru, že se jednalo o činnost nezávislých útočníků.[13] Mezi poslední zásadní událost lze zařadit ruské kybernetické útoky pokoušející se ovlivnit průběh amerických prezidentských voleb v roce 2016. Následkem bylo vyhoštěno 35 ruských diplomatů ze Spojených států amerických a zároveň byla uzavřena dvě ruská pracoviště.[14]

---

[8] *Tallinn manual on the international law applicable to cyber warfare*, 2013, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (accessed December 12, 2016), 106.

[9] NATO Cooperative Defense Centre of Excellence, "Cyber Definitions," 2016, https://ccdcoe.org/cyber-definitions.html (accessed December 12, 2016).

[10] Bryant Jordan, "US Still Has No Definition for Cyber Act of War," *Military.com*, 22. 6. 2016, http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html (accessed December 12, 2016).

[11] Michal Beránek and David Dvořák, "Kybernetické útoky v energetice," *SystemOnLine*, 2016, http://www.systemonline.cz/clanky/kyberneticke-utoky-v-energetice.htm (accessed December 11, 2016).

[12] Jana Čermáková, "Rusové na Krymu použili i kybernetické útoky, tvrdí šéf NBÚ," *Český rozhlas*, 5. 3. 2014, http://www.rozhlas.cz/zpravy/evropa/_zprava/podle-sefa-nbu-pouzili-rusove-na-krymu-i-kyberneticke-utoky--1323355 (accessed December 11, 2016).

[13] David Weissbrodt, "Cyber-Conflict, Cyber-Crime, and CyberEspionage," *Minnesota Journal of International Law*, vol. 22, 2013, http://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles, (accessed December 11, 2016), 349-350.

[14] "Žádné Američany za nové protiruské sankce nevyhostíme. Počkáme, až odejde Obama, řekl Putin," *Ihned.cz*, 29. 12. 2016, http://zahranicni.ihned.cz/amerika-usa/c1-65571540-spojene-staty-uvalily-na-rusko-sankce-za-hackersky-utok-pred-volbami-vyhostily-take-ruske-diplomaty (accessed January 1, 2017).

Jednotlivé typy hrozeb a jejich prostředí se samozřejmě vyvíjí v průběhu daného období. To, co dříve bylo považováno za nepravděpodobné, je v současné době možné charakterizovat i jako hrozbu s vysokou mírou rizika. Mezi hlavní důvody patří zvyšující se motivace útočníků, jejich nástroje, metody a nízké vstupní náklady. Navíc je velmi obtížná samotná identifikace daného útočníka (jedinec, organizovaná či neorganizovaná skupina, vláda, nestátní aktér),[15] který fakticky disponuje určitou anonymitou. Steven Stern dokonce uvádí, že anonymita pachatelů patří mezi hlavní problémy v kybernetickém prostoru.[16]

Kybernetické útoky mají různou podobu. Mezi nejčastější formy útoků v českém kybernetickém prostředí lze v současné době podle Vojenského zpravodajství zařadit „*metodu phishing a její sofistikovanější variantu spear phishing s využitím širokého spektra nejnovějších malware*.“[17] Mezi hlavní typy útočníků řadí vláda Spojeného království tzv. cyber criminals, konkurenty v průmyslu, zahraniční zpravodajské služby, hackery, hactivisty a zaměstnance. Mezi jejich motivaci můžeme zařadit: (1) zvýšení osobního ega; (2) finanční zisky; (3) získání obchodních výhod; (4) získání politických a ekonomických výhod pro danou zemi; či může sloužit jako (5) politický protest.[18]

3 Tvorba mezinárodního právního řadu v kybernetickém prostoru

Tvorba moderního mezinárodního práva v oblasti konfliktů sahá až do roku 1949, kdy byly přijaty Ženevské úmluvy (ŽÚ). Ty se tak staly, společně s dodatky z roku 1977, základními prameny válečného práva klasifikující čtyři kategorie konfliktů:[19]

1. Mezistátní konflikt - ozbrojený konflikt mezi státy včetně okupace (i částečné).
2. Národně osvobozenecká hnutí - boj proti okupaci, boj národů proti koloniálním a rasistickým režimům za sebeurčení.
3. Vnitrostátní konflikt - ozbrojený konflikt na území smluvní strany mezi jejími ozbrojenými silami a jinými organizovanými ozbrojenými skupinami majícími velení

[15] Cezar Vasilescu, ”Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. Století,” *Obrana a strategie*, vol. 1, 2012, http://www.obranaastrategie.cz/cs/archiv/rocnik-2012/1-2012/clanky/kyberneticke-utoky-nove-hrozby-pro-kritickou-informacni-infrastrukturu-ve-21-stoleti.html#4 (accessed December 14, 2016).

[16] ”The Steven E. Stern Workshop on Cyber-Terrorism - ICT16,” ICT, 2016, https://www.ict.org.il/Article/1852/the-steven-e-stern-workshop-on-cyber-terrorism-ict16 (accessed December 19, 2016), 13.

[17] Vojenské zpravodajství, ”VÝROČNÍ ZPRÁVA o činnosti Vojenského zpravodajství za rok 2015,” 2016, http://vzcr.cz/shared/clanky/20/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va_2015.pdf (accessed December 10, 2016), 15.

[18] ”Common Cyber Attacks: Reducing The Impact,” GCHQ a Cert-UK, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf (accessed December 10, 2016), 4.

[19] Marek Jukl, ”ŽENEVSKÉ ÚMLUVY A DODATKOVÉ PROTOKOLY (STRUČNÝ PŘEHLED),” Český červený kříž, 2005, http://www.cervenykriz.eu/cz/mhp/konvence.htm#A3 (accessed December 15, 2016).

a kontrolujícími část území, jež umožňuje provádět trvalé a koordinované vojenské operace a aplikovat ŽÚ. Nepatří sem izolované násilné činy, vnitřní nepokoje apod.

4. Ostatní ozbrojené konflikty - každý jiný ozbrojený konflikt na území smluvní strany.

Mezinárodní trestní tribunál pro bývalou Jugoslávii ve věci Tadić navíc rozvinul definici konfliktu, jenž nemá mezinárodní charakter, na *„déletrvající ozbrojené násilí mezi vládní autoritou a organizovanými ozbrojenými skupinami či mezi takovými skupinami uvnitř jednoho státu.“*[20] V oblasti kybernetických útoků však v mnoha případech nelze vždy zmíněná kritéria naplnit, jelikož útočníci mohou fungovat neorganizovaně a krátkodobě z jednoho či více oblastí. Nicméně jak bylo uvedeno v úvodní části statě, kybernetické útoky mají zejména mezinárodní povahu. Aby však mohl být kybernetický útok klasifikován jako mezinárodní ozbrojený konflikt, musí splňovat i podmínku “ozbrojenosti“. Kybernetické útoky jsou však v zásadním kontrastu vůči tradičnímu pojetí války a ozbrojených útoků. V současné době je mimo jiné velmi obtížné identifikovat daného útočníka či dokonce přičíst odpovědnost státu za útoky způsobené jednotlivci či skupinami, kteří nevykonávají činnost v rámci státních orgánů.[21] Na druhou stranu lze kybernetické útoky považovat za útoky, jelikož v praxi mohou způsobit nejen ekonomické škody, ale mohou například v případě útoků na kritickou infrastrukturu způsobit i zranění či smrt.[22]

Dalším problémem je, že doposud nebylo definováno, za jakých přesných podmínek lze považovat kybernetický útok pro použití síly dle čl. 2(4) Charty OSN, respektive klasifikace práva státu na obranu dle čl. 51 Charty OSN.[23] Například prof. Harold Hongju Koh v roce 2012 uvedl, že současné principy mezinárodního práva lze aplikovat pro kybernetický prostor a zároveň kybernetické aktivity mohou za určitých okolností představovat použití síly ve smyslu čl. 2(4) Charty OSN. Navíc uvedl, že je možné aplikovat i právo na sebeobranu podle čl. 51 Charty OSN.[24] Ke stejnému závěru došli i další odborníci

[20] International Committee of the Red Cross, ”How is the Term "Armed Conflict" Defined in International Humanitarian Law?,” 2008, https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (accessed December 20, 2016), 1.
[21] Michael Schmitt, ”Classification of Cyber Conflict.”
[22] Podle čl. 49 odst. 1 Dodatkového protokolu I k Ženevským úmluvám představují útoky násilné činy proti protivníkovi, a to jak útočné, tak i obranné.
[23] Článek 2 (4) Charty OSN stanovuje, že: „Členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly proti územní celistvosti nebo politické nezávislosti kteréhokoliv státu nebo jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů.“ Článek 51 stanovuje, že: „Nic v této chartě nesmí narušit přirozené právo na individuální nebo kolektivní sebeobranu, pokud dojde k ozbrojenému útoku proti členu Organizace spojených národů“.
[24] Harold Hongju Koh, ”International Law in Cyberspace,” *Harvard International Law Journal*, vol. 54, 2012, http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (accessed December 14, 2016).

včetně OSN, a to i přes to, že v článcích nejsou přímo doslovně uvedeny kybernetické útoky a tento závěr vyslovil i Mezinárodní soudní dvůr.[25] To, že současná podoba mezinárodního práva je aplikovatelná na kybernetické prostředí, bylo deklarováno i v Mezinárodní strategii pro kyberprostor Spojených států amerických[26] či například v samotném OSN reportu Group of Governmental Experts on Developments in the Field of Information and Telecommunications.[27]

Pro aplikování preventivního útoku je však nutné splnit několik podmínek: (1) útok musí mít proporcionální povahu vůči dané hrozbě; (2) užití ozbrojené síly musí být nezbytné, kdy dosažení míru není možné v dané situaci uskutečnit; a (3) musí se jednat o bezprostřední útok.[28] Jelikož se jedná zejména o tradiční vojenský instrument v reakci na útoky, které mají za následek lidskou oběť či poškození majetku, je aplikace čl. 51 Charty OSN v kybernetickém prostoru velmi těžko dosažitelná.[29] Tak jak uvedl Tim Maurer, mezinárodní normy v oblasti kybernetického prostoru jsou v současné době teprve ve fázi vzniku a bude nutné vytvořit mezinárodní právo kybernetického prostoru, kde budou začleněni nejen veškeří aktéři (např. soukromé společnosti, NGOs, apod.), ale zároveň vyřeší problematiku spojenou s přičitatelností samotných útoků,[30]a to například v případech, kdy bude nutná sebeobrana vůči nestátním aktérům na jednom či více územích, kdy hostitelský stát navíc nebude schopen sám učinit příslušné kroky.[31]

Například v září roku 2011 byl předložen návrh Mezinárodního kodexu chování pro informační bezpečnost ze strany Číny, Ruska, Tádžikistánu a Uzbekistánu, který by reguloval využívání informačních technologií v kybernetickém prostoru (v roce 2015 byla předložena aktualizovaná verze členskými státy Šanghajské organizace pro spolupráci - Čína,

[25] David Weissbrodt, "Cyber-Conflict, Cyber-Crime," 356.
[26] The White House, "INTERNATIONAL STRATEGY FOR CYBERSPACE: Prosperity, Security, and Openness in a Networked World," 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed December 11, 2016), 9.
[27] General Assembly, UN, "Developments in the field of information and telecommunications in the context of international security," 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E (accessed December 19, 2016), 2.
[28] Martin Horyna, "Krátký náhled na současnou problematiku kybernetických útoků," *PRÁVNÍ PROSTOR.CZ*, 29. 9. 2015, http://www.pravniprostor.cz/clanky/ostatni-pravo/kratky-nahled-na-soucasnou-problematiku-kybernetickych-utoku (accessed December 10, 2016) and David Weissbrodt, "Cyber-Conflict, Cyber-Crime," 364.
[29] David Weissbrodt, "Cyber-Conflict, Cyber-Crime," 364.
[30] Tomáš Flídr, "Mezinárodní právo kyberprostoru a Talinský manuál," *Kyberbezpečnost.cz*, 22. 11. 2013, https://www.kyberbezpecnost.cz/?p=198 (accessed December 19, 2016).
[31] Chatham House, "Classification of Conflicts: The Way Forward," 2012, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/011012summary.pdf (accessed December 10, 2016).

Rusko, Kazachstán, Kyrgyzstán, Tádžikistán a Uzbekistán). Tyto regulace by podle některých expertů mohly být srovnatelné například s Úmluvou o zákazu používání chemických zbraní z roku 1992. Na druhou stranu tento kodex vyvolává obavy z důvodu porušování lidských práv a s možností, že se opět nesetká s globální podporou.[32] V současné době tak zůstává teoretickým dokumentem snažícím se o mezinárodní úpravu chování v kybernetickém prostoru tzv. Tallinnský manuál o mezinárodním právu aplikovatelném na válku v kyberprostoru.

Co se týče aplikace čl. 39 a 41,[33] ty se vztahují na politické rozhodnutí reagovat na daný útok. Možné opatření může být však vetováno jakoukoliv členskou zemí Rady bezpečnosti. Z toho důvodu je teoreticky vyšší pravděpodobnost reakce daného státu vůči jednotlivým útokům bez souhlasu Rady bezpečnosti (sebeobrana), a to včetně možnosti porušení mezinárodního práva. Lze tedy spíše očekávat, že komplexní multilaterální nástroje řešící tuto problematiku budou postupně vznikat z národních praxí a reakcí na jednotlivé kybernetické útoky.

4 NATO a kybernetická obrana

Zárodky při budování určitých norem je možné shledat v rozvoji kolektivní kybernetické obrany a ochrany mezi členskými státy NATO. Hlavní impuls k rozvoji kolektivní kybernetické obrany a ochrany kritické infrastruktury se staly zmíněné kybernetické útoky v Estonsku. Nicméně již v roce 2002 během Summitu NATO v Praze se upozorňovalo na potřebu posílit kybernetickou obranu a například bylo doporučeno založit Cyber Defense Program. Samotný kybernetický útok v Estonsku pak již pouze v praxi odhalil nedostatky v aktivitách NATO v oblasti kybernetické bezpečnosti.[34]

V roce 2008 tak byl zřízen Cooperative Cyber Defense Centre NATO of Excellence v Tallinnu (Estonsko), v roce 2010 byly kybernetické útoky zahrnuty mezi významné hrozby v samotné Strategické koncepci NATO a v roce 2011 byla schválena NATO Policy on Cyber

[32] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," 2015, https://citizenlab.org/2015/09/international-code-of-conduct/ (accessed December 12, 2016) and CCDCOE, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?," 2015, https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html (accessed December 10, 2016).

[33] Čl. 39 a 41, který umožnuje přijmout Radě bezpečnosti opatření leteckou, námořní či pozemní silou pro udržení nebo obnovení mezinárodního míru a bezpečnosti.

[34] David P. Fidler, Richard Pregent and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Articles by Maurer Faculty*, 2013, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (accessed December 14, 2016), 5.

Defense.[35] V roce 2014 během Summitu ve Walsu se členské země zavázaly k možnosti aktivovat čl. 5 Washingtonské smlouvy vůči kybernetickým útokům a během posledního Summitu ve Varšavě v roce 2016 byl kybernetický prostor deklarován jako další operační oblast vedle země, vzduchu, vody a vesmíru.[36] Reakce NATO a aliančních zemí na prohlubující se hrozby v oblasti kybernetické bezpečnosti, jsou pochopitelné, a to zejména vzhledem ke globálnímu charakteru této problematiky.[37]

V současné době však nelze spoléhat pouze na bezpečnostní záruky v rámci aktivace čl. 5 Washingtonské smlouvy, jelikož ten automaticky negarantuje vojenskou pomoc, a navíc byl v historii aktivován pouze jednou na základě teroristických útoků v USA 11. září 2001. Cílem článku je „*udržet a obnovit bezpečnost v severoatlantickém prostoru*“,[38] a to za pomocí nezbytně nutných úkonů. Generální tajemník NATO Jens Stoltenberg mimo jiné uvedl, že tento článek bude aktivován pouze v případě, pokud se bude jednat o rozsáhlý útok, kdy bude možné identifikovat konkrétního aktéra (stát či jednotlivec nebo organizace podporovaná státem).[39] Aktivace článku je totiž vázáná vždy mezinárodním právem (právo na individuální nebo kolektivní obranu uznané čl. 51 Charty OSN). V praxi to tedy znamená, že Aliance je nucena harmonizovat své kroky nejen se zájmy členských zemí a jejich vnitrostátním právem, které se ve většině případů navíc řídí i nadnárodním právem EU, ale zejména mezinárodním právem.[40] To se však nevztahuje na veškeré kybernetické útoky a na veškeré aktéry v kybernetickém prostoru. Pokud bude tedy například chtít NATO řešit i trestněprávní aktivity, jako například špionáže, bude muset překročit rámec své působnosti. V praxi to však bude znamenat rozvinutí kybernetické obrany ve třech hlavních oblastech: (1) větší dohled jednotlivých vlád nad informačními systémy; (2) nutnost sdílení informací, a to jak ze strany státních aktérů, tak i nestátních; (3) aktivní obrana.[41]

Úloha NATO může být v budoucnu klíčová, jelikož členové mají podobné zájmy. Na druhou stranu bude zejména záležet na přístupu členských zemí a možnosti vytvořit vlastní obrannou kapacitu v oblasti kybernetické bezpečnosti. Jen tak bude totiž možné reagovat včas na danou akci protivníka. Navíc bude důležité, zdali bude existovat vůle pro

[35] Cezar Vasilescu, ”Kybernetické útoky.”
[36] NATO, ”Warsaw Summit Communiqué,” 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed 10. 12. 2016).
[37] Zdeněk Kříž, ”Rozšiřování Severoatlantické aliance a jeho vliv na bezpečnost nových členů,” *Politologický časopis*, vol. 1, 1998, https://is.muni.cz/publication/561862 (accessed December 19, 2016), 1.
[38] Zdeněk Kříž, ”Rozšiřování Severoatlantické aliance”, 44.
[39] Vladimír Bízik, ”Kyberprostor: nová fronta NATO,” 19. 7. 2016, http://www.evropskehodnoty.cz/kyberprostor-nova-fronta-nato/ (accessed December 10, 2016).
[40] David P. Fidler, Richard Pregent and Alex Vandurme, ”NATO, Cyber Defense,” 13.
[41] Ibid., 18-19.

rozšíření svého statutu působnosti, tedy za rámec kolektivní obrany, aby byla schopna čelit hrozbám v následujících desetiletích. Národní vlády budou zároveň stát před zásadním politickým problémem, a to jakým způsobem budou omezovány základní občanské svobody možnými legislativními opatřeními pro eliminaci jednotlivých hrozeb.

5 Role národních vlád a příklad České republiky

Hlavním problémem v aplikaci mezinárodního práva na obranu států vůči kybernetickým útokům je nepřipravenost. To se mimo jiné ukázalo během kybernetických útoků v roce 2007 v Estonsku a o rok později v Gruzii. Mezi další problémy patří neomezená geografická vzdálenost, vysoká míra anonymity jednotlivých aktérů, velmi rychlý rozvoj technologií a specifikum samotných útoků. Z toho důvodu je nutná tvorba legislativního rámce a prevence proti kybernetickým útokům na národní úrovni.

Změny jsou viditelné nejen v legislativních opatřeních přijatých světovými velmoci, ale například i Českou republikou. V roce 2011 zařadil Úřad vlády České republiky v Bezpečnostní strategii kybernetické útoky mezi hlavní hrozby, které ohrožují strategické zájmy země. V témže roce mimo jiné došlo ke zřízení Národního centra kybernetické bezpečnosti a v následujících letech bylo schváleno několik zásadních legislativních opatření:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti;
- nařízení vlády č. 315/2014, kterým se změnilo nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury;
- vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti;
- vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

Mezi hlavní milníky patří i publikace strategických dokumentů (Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, Akční plán kybernetické bezpečnosti České republiky na období let 2015 až 2020) či uzavření mezistátních dohod.[42] V současné době však není v zákonech přisouzena odpovědnost pro zajištění kybernetické obrany jakémukoliv státnímu úřadu. To by se mělo však změnit novelou zákona č. 289/2005 Sb. o Vojenském zpravodajství, která by tuto oblast měla přidělit

[42] Luděk Jiráček, "Cyber security threats," 65.

Vojenskému zpravodajství. Ten aktuálně prošel prvním čtením. Mezi další úkoly Vojenského zpravodajství má podle novely patřit předcházení, zastavení nebo odvrácení kybernetického útoku včetně možnosti využití prostředků k odposlechům.[43] Vojenské zpravodajství je také posvěceno vybudováním Národního centra kybernetických sil.[44]

Národní vlády členských zemí Evropské unie, včetně České republiky, jsou také vázány jednotlivými směrnicemi a nařízeními z nadnárodní úrovně. Dne 6. července 2016 byla Evropským parlamentem schválená směrnice věnovaná kybernetické bezpečnosti (Network and Information Security), jejímž cílem je standardizovat úroveň bezpečnostních sítí a informačních systémů. Ta byla publikována v Úředním věštníku 19. července 2016 a musí být implementována členskými zeměmi do 21 měsíců.[45]

6 Tvorba mezinárodního právního řadu v oblasti AI

AI a věda zabývající se touto problematikou je velmi komplexní a stále poměrně mladou disciplínou. Teprve v roce 2013 se například začala oblast autonomních zbraní projednávat na neformální úrovni na půdě OSN, respektive v rámci Úmluvy o zákazu nebo omezení použití některých konvenčních zbraní.[46] Na hrozby spojené se zneužitím autonomních zbraní upozorňují však nejen neziskové organizace, jako například Stop Killer Robots, ale zejména přední vědci.[47]

Pro definici umělé inteligence je velmi často užívaná definice z roku 1967 (Marvin Minsky), která klasifikuje AI jako „*vědu o vytváření strojů nebo systémů, které budou při řešení určitého úkolu užívat takového postupu, který - kdyby ho dělal člověk - bychom považovali za projev jeho inteligence*“.[48] E. Richová se domnívá, že “*umělá inteligence se zabývá tím, jak počítačově řešit úlohy, které dnes zatím zvládají lidé lépe*.“ Umělá inteligence je však obsáhlou vědní disciplínou, která se rozděluje na několik hlavních podkategorií a metod, a to například na: (1) expertní systémy; (2) genetické algoritmy;

[43] Poslanecká sněmovna Parlamentu České republiky, ”Sněmovní tisk 931 - Novela z. o Vojenském zpravodajství,” 2013, https://www.psp.cz/sqw/historie.sqw?o=7&t=931 (accessed January 1, 2017).
[44] Luděk Jiráček, ”Cyber security threats,” 63.
[45] Národní bezpečnostní úřad, ”Návrh na změnu zákona o kybernetické bezpečnosti - transpozice směrnice NIS,” 21. 7. 2016, https://www.nbu.cz/cs/aktuality/626-navrh-na-zmenu-zakona-o-kyberneticke-bezpecnosti---transpozice-smernice-nis/ (accessed January 1, 2017).
[46] Vincent Boulanin, ”Implementing Article 36 weapon reviews in the light of increasing autonomy in weapon systems,” *SIPRI Insights on Peace and Security*, vol. 1, 2015, https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1501.pdf (accessed January 3, 2017), 1.
[47] Luděk Jiráček, ”Umělá inteligence a tvorba legislativního rámce,” *natoaktual.cz*, 17. 10. 2016, http://www.natoaktual.cz/umela-inteligence-a-tvorba-legislativniho-ramce-ft5-%20/na_analyzy.aspx?c=A161017_151929_na_analyzy_m02 (accessed December 19, 2016).
[48] Pavel Vachtl, ”24. ledna 2016 zemřel Marvin Minsky, jeden z otců umělé inteligence,” *Český rozhlas*, 29. 1. 2016, http://www.rozhlas.cz/leonardo/technika/_zprava/24-ledna-2016-zemrel-marvin-minsky-jeden-z-otcu-umele-inteligence--1579051 (accessed January 3, 2017).

(3) multiagentní sítě; či (4) umělé neuronové sítě.[49] Navíc je možné se setkat s AI i v netechnických oborech jako jsou například lingvistika, psychologie či filosofie.[50]

6.1 Zavedení legislativních opatření (ex-ante vs. ex-post)

Jednotná a univerzální definice neexistuje a konsensus na tom, co by mělo být přesně regulováno či dokonce jak by daný problém měl být regulován, v současné době také neexistuje. Navíc ani nelze naleznout shoda na jednotné kontrole nad mezinárodním obchodem se zbraněmi. Doposud byla tzv. Arms Trade Treaty ratifikována pouze 88 státy a světové velmoci (př. USA, Čína, Indie, Rusko) smlouvu doposud ani neratifikovaly.[51]

Výrazné investice do AI v současné době však probíhají nejen v soukromém sektoru, ale i veřejném, respektive v obranném průmyslu. To potvrzuje i předseda představenstva britské zbrojovky BAE Rogera Carra, podle kterého se snaží vyvíjet autonomní roboty s cílem zabíjet více než 40 zemí. Výrazné investice v soukromém sektoru potvrzují i nejvýznamnější soukromé společnosti, jako například Google, Microsoft či Facebook. Jelikož využití AI skrývá nejen významný potenciál, ale i značná bezpečnostní rizika, přední vědci doporučují zavést určitá regulační opatření proti zneužití a používání AI zejména v obranném průmyslu.[52]

Tak jak je možná aplikace mezinárodní práva v oblasti kybernetické bezpečnosti diskutabilní, u využití AI v ozbrojených konfliktech tomu není a v krátkodobém horizontu ani s největší pravděpodobností nebude jinak. Mezi hlavními možnými teoretickými otázkami, jež se budou v rámci mezinárodní práva klást, bude patřit, zdali plně automatizované systémy budou vůbec schopny dodržovat mezinárodní principy v ozbrojeném konfliktu, jako například princip proporcionality, necílení na civilní obyvatelstvo a civilní objekty. Otázkou také bude, zdali bude lidský operátor vůbec schopen pochopit daný systém a bude mít možnost ověřit, zdali takovýto systém bude schopen vykonávat určitý úkon v souladu s mezinárodním právem.[53] Navíc bude nutné nastavit adekvátní vztah s lidským operátorem, respektive zdali bude nastavená určitá ochrana a možnost potlačit robotické rozhodnutí.[54] V oblasti kontroly ex-ante je tedy zásadní kontrola již při navrhování daného algoritmu. Z toho důvodu se

[49] Luděk Jiráček, "Umělá inteligence a tvorba legislativního rámce."
[50] Management Mania, "Umělá inteligence (Artificial intelligence)," *ManagementMania*, Last modified December 12, 2015, https://managementmania.com/cs/umela-inteligence (accessed December 17, 2016).
[51] UNODA, "The Arms Trade Treaty," https://www.un.org/disarmament/convarms/att/ (accessed January 1, 2017).
[52] Luděk Jiráček, "Změní umělá inteligence bezpečnostní politiku států a mezinárodní vztahy?," *natoaktual.cz*, 8. 8. 2016, http://www.natoaktual.cz/zmeni-umela-inteligence-bezpecnostnipolitiku-statu-a-mezinarodni-vztahy-1uc-%20/na_analyzy.aspx?c=A160808_105816_na_analyzy_m02 (accessed December 19, 2016).
[53] Vincent Boulanin, "Implementing Article 36," 11.
[54] Ibid., 12.

například v současné době společnost GoogleMind snaží s předními experty nalézt způsob, jak deaktivovat daný autonomní systém bez toho, aby se dozvědělo o deaktivačním zásahu.[55]

K tomu, aby vznikla určitá shoda pro zavedení univerzálně a právně závazné mezinárodní smlouvy pro regulaci zbrojení, včetně nastavení etických pravidel, je nutná také určitá důvěra a shoda mezi danými aktéry a subjekty.[56] Mezinárodní vztahy jsou však založeny na nedůvěře. Každý aktér mezinárodních vztahů včetně jednotlivých subjektů v soukromém sektoru bude mít zájem si zachovat konkurenční výhodu či dokonce ji využít pro dosažení stanovených cílů – zvýšení obchodních zisků, udržení a posílení pozic v mezinárodních vztazích, apod.[57] Další problematikou může být například určení zodpovědnosti za uskutečnění útoku, který nebude v souladu s mezinárodním právem (výrobce, programátor, velitel akce?) a zabránění náhodnému zneužití či selhání systémů.

Zavedení určité regulace během vývoje je však více než spekulativní, a to zejména kvůli diskrétnosti a značné utajovanosti jednotlivých výzkumných fází vývoje. I kdyby se zavedly určité kontrolní mechanismy, problémem bude zmíněný rychlý vývoj nových technologií, díky kterému budou muset být kontrolní mechanismy pravidelně upravovány. Navíc takovéto kontroly jsou technicky náročné a velmi finančně nákladné. Určitá kontrola nových zbraní, zbraňových systémů a nový způsob vedení válečných konfliktů, je například již obsažena v článku 36 Dodatkového protokolu I z roku 1977 ŽÚ, kdy je přímo uložena povinnost států provést právní přezkum, zdali je využití nových zbraní a zbraňových systémů v souladu s mezinárodním právem. To je však i v případě využití kybernetických zbraní v současné době stále otevřeným tématem.[58] Navíc samotný mechanismus přezkumu není jednotný a v každé zemi se tak může lišit.[59] Lze tedy očekávat, tak jako u kybernetických hrozeb, že možná legislativní opatření na globální úrovni budou tvořena v okamžiku, kdy bude hmatatelná hrozba.

[55] Computerworld.cz, "Robotiční tyrané? Terminátoři? Umělá inteligence dostane „červené tlačítko". Google připravuje Kill switch," *Computerworld*, 8. 6. 2016, http://computerworld.cz/technologie/roboticni-tyrane-terminatori-umela-inteligence-dostane-cervene-tlacitko-google-pripravuje-kill-switch-53108 (accessed December 19, 2016).
[56] Jan Ondřej, "Odzbrojení a regulace zbrojení v mezinárodním právu a ve vztahu k suverenitě státu," *Mezinárodní vztahy*, vol. 34, 1999, https://mv.iir.cz/article/download/1203/1252 (accessed December 19, 2016), 60.
[57] Luděk Jiráček, "Změní umělá inteligence bezpečnostní politiku států a mezinárodní vztahy?."
[58] Vincent Boulanin, "Implementing Article 36," 4.
[59] Ibid., 7.

Závěr

Aplikace mezinárodního práva se díky rozvoji nových technologií ukazuje jako problematická, a to i přes to, že řada expertů se shoduje na možnosti uplatňování aktuální podoby mezinárodního práva na řešení konfliktů v kybernetickém prostoru. Teoreticky a v omezených případech tomu opravdu je. Prakticky však nikoliv. Veškeré bezpečnostní hrozby globálního charakteru, včetně jejich definic, jsou totiž vnímané a chápané jednotlivými civilizacemi odlišně. Mimoto jsou mezinárodní vztahy založeny na nedůvěře a často značném neporozumění. V současné době nepanuje ani shoda na tom, co a jak má být přesně regulováno.

V praxi bude také problematické nastavit určité kontrolní mechanismy, jelikož jednotlivé vlády nebudou mít zájem o sledování sítí a systémů třetí stranou, respektive kontroly dodržování stanovených závazků. Nelze ani očekávat, že jednotlivé velmoci budou mít zájem o ztrátu komparativní výhody při řešení jednotlivých mezistátních konfliktů, které se v kybernetickém prostoru nabízí (př. podniknutí vojenské intervence bez použití lidské síly, vysoká míra utajení, apod.). Z toho důvodu není možné očekávat, že se v krátkodobém až střednědobém horizontu zavedou jednotné, komplexní a funkční normy na globální úrovni, a to jak pro řešení konfliktů v kybernetickém prostoru, tak i pro možné využívání plně automatizovaných zbraní. Ty budou spíše postupně vznikat z národních praxí a reakcí na jednotlivé kybernetické útoky a na samotnou činnost AI.

Z výše uvedených důvodů je nutné zajistit spolehlivost a bezpečnost kritické infrastruktury na národní úrovni včetně snahy zabraňovat špionážním kybernetickým útokům vůči osobním údajům a datům. Možné legislativní kroky budou však stát před zásadním politickým problémem, a to, jakým způsobem budou omezovány základní občanské svobody pro eliminaci daných hrozeb. Ty mohou však být částečně eliminovány i díky zvýšení gramotnosti obyvatelstva v oblasti kybernetické bezpečnosti. Dalším zásadním problémem je nedostatek odborníků ve veřejném sektoru. Pokud jim stát nebude schopen zajistit konkurenceschopné pracovní podmínky, budou nadále působit v soukromém sektoru.

Zároveň je na místě veřejně deklarovat snahu o spolupráci na mezinárodní úrovni v oblasti možných kybernetických protiútoků vůči nepřátelům. To však bude možné pouze za podmínky propojení veřejného a soukromého sektoru mezi jednotlivými zeměmi například v oblasti informování o kybernetických útocích včetně možnosti rozšíření statutu působnosti Severoatlantické aliance za rámec kolektivní obrany. Navíc díky hybridní podobě konfliktů, které se neuskutečňují pouze na operační úrovni, bude nutné, aby národní vlády

a mezinárodní organizace byly schopny reagovat na novodobou podobu konfliktů aktivněji, příměji, flexibilněji a efektivněji.

Soupis literatury

Beránek, Michal and Dvořák, David. "Kybernetické útoky v energetice," *SystemOnLine*, 2016, http://www.systemonline.cz/clanky/kyberneticke-utoky-v-energetice.htm (accessed December 11, 2016).

Bízik, Vladimír. "Kyberprostor: nová fronta NATO," 19. 7. 2016, http://www.evropskehodnoty.cz/kyberprostor-nova-fronta-nato/ (accessed December 10, 2016).

Boulanin, Vincent. "Implementing Article 36 weapon reviews in the light of increasing autonomy in weapon systems," *SIPRI Insights on Peace and Security*, vol. 1, 2015, https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1501.pdf (accessed January 3, 2017).

CCDCOE. "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?," 2015, https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html (accessed December 10, 2016).

Computerworld.cz. "Robotiční tyrané? Terminátoři? Umělá inteligence dostane „červené tlačítko". Google připravuje Kill switch," *Computerworld*, 8. 6. 2016, http://computerworld.cz/technologie/roboticni-tyrane-terminatori-umela-inteligence-dostane-cervene-tlacitko-google-pripravuje-kill-switch-53108 (accessed December 19, 2016).

Čermáková, Jana. "Rusové na Krymu použili i kybernetické útoky, tvrdí šéf NBÚ," *Český rozhlas*, 5. 3. 2014, http://www.rozhlas.cz/zpravy/evropa/_zprava/podle-sefa-nbu-pouzili-rusove-na-krymu-i-kyberneticke-utoky--1323355 (accessed December 11, 2016).

Fidler, David P. Pregent, Richard and Vandurme, Alex. "NATO, Cyber Defense, and International Law," *Articles by Maurer Faculty*, 2013, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (accessed December 14, 2016).

Flídr, Tomáš. "Mezinárodní právo kyberprostoru a Talinský manuál," *Kyberbezpečnost.cz*, 22. 11. 2013, https://www.kyberbezpecnost.cz/?p=198 (accessed December 19, 2016).

General Assembly, UN. "Developments in the field of information and telecommunications in the context of international security," 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E (accessed December 19, 2016).

GCHQ and Cert-UK. "Common Cyber Attacks: Reducing The Impact," 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf (accessed December 10, 2016).

Horyna, Martin. ”Krátký náhled na současnou problematiku kybernetických útoků,” *PRÁVNÍ PROSTOR.CZ*, 29. 9. 2015, http://www.pravniprostor.cz/clanky/ostatni-pravo/kratky-nahled-na-soucasnou-problematiku-kybernetickych-utoku (accessed December 10, 2016).

Chatham House. ”Classification of Conflicts: The Way Forward,” 2012, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/011012summary.pdf (accessed December 10, 2016).

ICT. ”The Steven E. Stern Workshop on Cyber-Terrorism - ICT16,” 2016, https://www.ict.org.il/Article/1852/the-steven-e-stern-workshop-on-cyber-terrorism-ict16 (accessed December 19, 2016).

International Committee of the Red Cross. ”How is the Term "Armed Conflict" Defined in International Humanitarian Law?,” 2008, https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (accessed December 20, 2016).

Jiráček, Luděk. ”Cyber security threats: the case of the Czech Republic,” in *Poland, the Czech Republic and NATO in Fragile Security Contexts*, edited by Anna Visvizi and Tomasz Stępniewski, 2016, http://www.amo.cz/wp-content/uploads/2016/12/Poland-the-Czech-Republic-and-NATO-in-Fragile-Security-Contexts.pdf (accessed December 16, 2016).

Jiráček, Luděk. ”Umělá inteligence a tvorba legislativního rámce,” *natoaktual.cz*, 17. 10. 2016, http://www.natoaktual.cz/umela-inteligence-a-tvorba-legislativniho-ramce-ft5-%20/na_analyzy.aspx?c=A161017_151929_na_analyzy_m02 (accessed December 19, 2016).

Jiráček, Luděk. ”Změní umělá inteligence bezpečnostní politiku států a mezinárodní vztahy?,” *natoaktual.cz*, 8. 8. 2016, http://www.natoaktual.cz/zmeni-umela-inteligence-bezpecnostnipolitiku-statu-a-mezinarodni-vztahy-1uc-%20/na_analyzy.aspx?c=A160808_105816_na_analyzy_m02 (accessed December 19, 2016).

Jirásek, Petr. Novák, Luděk and Požár, Josef. ”Výkladový slovník kybernetické bezpečnosti,” Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2013, https://www.govcert.cz/download/aktuality/container-nodeid-548/slovnikv231nbuwebcolor.pdf (accessed 10. 12. 2016).

Jordan, Bryant. ”US Still Has No Definition for Cyber Act of War,” *Military.com*, 22. 6. 2016, http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html (accessed December 12, 2016).

Jukl, Marek. ”ŽENEVSKÉ ÚMLUVY A DODATKOVÉ PROTOKOLY (STRUČNÝ PŘEHLED),” Český červený kříž, 2005, http://www.cervenykriz.eu/cz/mhp/konvence.htm#A3 (accessed December 15, 2016).

Koh, Harold Hongju. ”International Law in Cyberspace,” *Harvard International Law Journal*, vol. 54, 2012, http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (accessed December 14, 2016).

Kříž, Zdeněk. ”Rozšiřování Severoatlantické aliance a jeho vliv na bezpečnost nových členů,” *Politologický časopis*, vol. 1, 1998, https://is.muni.cz/publication/561862 (accessed December 19, 2016).

Management Mania. ”Umělá inteligence (Artificial intelligence),” *ManagementMania*, Last modified December 12, 2015, https://managementmania.com/cs/umela-inteligence (accessed December 17, 2016).

McKune, Sarah. ”An Analysis of the International Code of Conduct for Information Security,” 2015, https://citizenlab.org/2015/09/international-code-of-conduct/ (accessed December 12, 2016).

Národní bezpečnostní úřad, ”Návrh na změnu zákona o kybernetické bezpečnosti - transpozice směrnice NIS,” 21. 7. 2016, https://www.nbu.cz/cs/aktuality/626-navrh-na-zmenu-zakona-o-kyberneticke-bezpecnosti---transpozice-smernice-nis/ (accessed January 1, 2017).

NATO Cooperative Defense Centre of Excellence. ”Cyber Definitions,” 2016, https://ccdcoe.org/cyber-definitions.html (accessed December 12, 2016).

NATO. ”Warsaw Summit Communiqué,” 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed 10. 12. 2016).

Ondřej, Jan. ”Odzbrojení a regulace zbrojení v mezinárodním právu a ve vztahu k suverenitě státu,” *Mezinárodní vztahy*, vol. 34, 1999, https://mv.iir.cz/article/download/1203/1252 (accessed December 19, 2016).

Pavlíková, Miroslava. ”KYBERNETICKÝ BOJ MEZI RUSKEM A UKRAJINOU V RÁMCI UKRAJINSKÉHO KONFLIKTU,” *Obrana a strategie*, vol. 1, 2016, http://www.obranaastrategie.cz/cs/archiv/rocnik-2016/1-2016/clanky/kyberneticky-boj-mezi-ruskem-a-ukrajinou-v-ramci-ukrajinskeho-konfliktu.html#13 (accessed December 10, 2016).

Poslanecká sněmovna Parlamentu České republiky, ”Sněmovní tisk 931 - Novela z. o Vojenském zpravodajství,” 2013, https://www.psp.cz/sqw/historie.sqw?o=7&t=931 (accessed January 1, 2017).

Schmitt, Michael. ”Classification of Cyber Conflict,” *Journal of Conflict and Security Law*, 2012, 17 (2), http://jcsl.oxfordjournals.org/content/17/2/245.full#xref-fn-18-1 (accessed 10. 12. 2016).

Tallinn manual on the international law applicable to cyber warfare, 2013, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (accessed December 12, 2016).

The White House. ”INTERNATIONAL STRATEGY FOR CYBERSPACE: Prosperity, Security, and Openness in a Networked World,” 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed December 11, 2016).

UNODA. ”The Arms Trade Treaty,” https://www.un.org/disarmament/convarms/att/ (accessed January 1, 2017).

Vachtl, Pavel. ”24. ledna 2016 zemřel Marvin Minsky, jeden z otců umělé inteligence,” *Český rozhlas*, 29. 1. 2016, http://www.rozhlas.cz/leonardo/technika/_zprava/24-ledna-2016-zemrel-marvin-minsky-jeden-z-otcu-umele-inteligence--1579051 (accessed January 3, 2017).

Vasilescu, Cezar. ”Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. Století,” *Obrana a strategie*, vol. 1, 2012, http://www.obranaastrategie.cz/cs/archiv/rocnik-2012/1-2012/clanky/kyberneticke-utoky-nove-hrozby-pro-kritickou-informacni-infrastrukturu-ve-21-stoleti.html#4 (accessed December 14, 2016).

Vojenské zpravodajství. ”VÝROČNÍ ZPRÁVA o činnosti Vojenského zpravodajství za rok 2015,” 2016, http://vzcr.cz/shared/clanky/20/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va_2015.pdf (accessed December 10, 2016).

Weissbrodt, David. ”Cyber-Conflict, Cyber-Crime, and CyberEspionage,” *Minnesota Journal of International Law*, vol. 22, 2013, http://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles, (accessed December 11, 2016).

”Žádné Američany za nové protiruské sankce nevyhostíme. Počkáme, až odejde Obama, řekl Putin,” *Ihned.cz*, 29. 12. 2016, http://zahranicni.ihned.cz/amerika-usa/c1-65571540-spojene-staty-uvalily-na-rusko-sankce-za-hackersky-utok-pred-volbami-vyhostily-take-ruske-diplomaty (accessed January 1, 2017).