Právní aspekty kybernetické bezpečnosti ČR

Jakub Harašta

Úvod **66**
1. Informační společnost a její bezpečnost **66**
1.1 Pojem a znaky informační společnosti 66
1.2 Informační sebeurčení 69
1.3 Povaha kybernetické bezpečnosti 72
2. Hrozby a nástroje ochrany **76**
2.1 Změny bezpečnostních hrozeb 76
2.2 Prostředky ochrany 80
3. Úprava kybernetické bezpečnosti v jednotlivých zemích **82**
3.1 Kybernetická bezpečnost ve vyspělých zemích 82
3.2 Kybernetická bezpečnost ve střední a východní Evropě 86
Závěr: Česká republika **88**
Seznam použitých pramenů **89**

Právní aspekty kybernetické bezpečnosti ČR

Abstrakt

Tento článek se zabývá specifikací východisek kybernetické bezpečnosti v současné společnosti. Zároveň konstatuje důležitost a potřebnost konsistentního přístupu ke kybernetické bezpečnosti za předpoklad respektu k informačnímu sebeurčení, které představuje klíčovou hodnotu formulovanou informační společností. Práce nejdříve dle dostupné literatury hledá konsensus na obsahu pojmu kybernetické bezpečnosti tak, aby reflektoval současný vývoj informační společnosti, a tato východiska potom konfrontuje s úpravou kybernetické bezpečnosti ve vyspělých státech. Práce předkládá bodový přehled zásadních cílů, ke kterým by měla směřovat nová legislativa v ČR a v jí podobných mladých demokraciích.

Klíčová slova

kybernetická bezpečnost, informační a komunikační technologie, informační sebeurčení, Česká republika, kritické informační infrastruktury

Abstract

This papers deals with the specification of premises of the cyber security in contemporary society. At the same time it notes great importance and necessity of consistent approach toward the cyber security, compliant with the information self-determination, which presents the key value articulated by the information society. The first part includes literature analysis and searches for consensus of cybernetic security in such way to reflect current development of information society and these premises are confronted with legislation in developed states. The list of basic goals to which the new legislation of Czech Republic and all the similar young democratic states should aim is also articulated.

Keywords

cybersecurity, information and communication technologies, informational self-determination, the Czech Republic, critical information infrastructures

Mgr. Jakub Harašta

harasta.jakub@gmail.com

Jakub Harašta získal v roce 2013 magisterský titul v oboru Právo a právní věda na Právnické fakultě Masarykovy univerzity. V průběhu studia absolvoval výměnný pobyt na Mykolo Romerio Universitetas v litevském Vilniusu, odbornou stáž na Velvyslanectví České republiky tamtéž a odbornou stáž v advokátní kanceláři Valterse Gencse v lotyšské Rize. Momentálně působí na své alma mater jako asistent a pokračuje v doktorském studiu v oboru Práva informačních a komunikačních technologií. Od července 2013 také působí jako advokátní koncipient v kanceláři Mgr. Michala Grubera v Brně, kde se zabývá zejména insolvenční a obchodněprávní agendou.

Úvod

Informační sítě představují pro dnešní společnost kriticky důležité struktury, které umožňují sdílet obrovské množství informací ve zlomku sekundy. Funkce informačních sítí je natolik důležitá, že kromě jejich svobody musí být zajištěna i jejich funkčnost. Náležitá pozornost tak musí být věnována kybernetické bezpečnosti, což se ale často neděje. Jednotlivci, korporace i státy se v prostředí informačních sítí často chovají až neskutečně zbrkle a ignorují nové druhy nebezpečí plynoucí z informační společnosti.

Tato práce se věnuje právním aspektům kybernetické bezpečnosti České republiky s důrazem na porovnání stavu oproti státům vyspělým i státům České republice do určité míry podobným. Zároveň se ale snaží konstruovat kybernetickou bezpečnost tak, jak konstruována být musí – jako nedistributivní právo chránící konkrétní distributivní práva plynoucí z konkrétního stavu společnosti. Nástroje prosazující kybernetickou bezpečnost bez tohoto širšího chápání souvislostí, a bez respektu k informačnímu sebeurčení, mohou napáchat více škody, než kybernetické útoky samotné. Mohou omezit schopnost internetu fungovat jako svobodné a globální médium, mohou usnadnit nadměrné sledování uživatelů jednotlivých informačních sítí atd. Práce tedy prostřednictvím kvalitativních i kvantitativních změn popisuje informační společnost, aby dále sledovala současné bezpečnostní hrozby v ní se objevující, včetně specifikace obecných trendů. Nakonec dochází k porovnání úpravy kybernetické bezpečnosti ve vyspělých státech (Německo, Spojené království, USA) a ve státech nám společensky blízkých (Visegrádská čtyřka, Pobaltské státy). Cílem je uchopení plánované české legislativy v této oblasti (tedy Návrhu zákona o kybernetické bezpečnosti) v širších společenských souvislostech. Dále je cílem za použití pragmatické metody zhodnotit, zdali reflektuje současný vývoj na poli kybernetické bezpečnosti v rámci obecných právních i bezpečnostních otázek, a zdali je možné jej porovnat s obdobnými úpravami v zahraničí, ať se již jedná o přístupy vyspělých států nebo nám blízkých zemí v kontinentální Evropě.

1. Informační společnost a její bezpečnost

1.1 Pojem a znaky informační společnosti

Přirozenou tendencí společnosti je rozvoj k vyšší míře informovanosti.[1] Společnost tedy v minulosti využívala technologického pokroku umožňujícího zrychlenou výměnu informací ke své vlastní evoluci. Zatím posledním vývojovým krokem na poli rychlosti výměny informací je masivní proliferace informačních technologií do běžného života společnosti. Rozšíření informačních technologií dosáhlo takové míry, že je možné mluvit o fundamentální změně způsobu socializace či obchodu.[2] V návaznosti jsme pak svědky rozvoje síťových organizačních modelů (nahrazujících klasická hierarchická uspořádání),[3] výskytu a rozvoje participativní složky nahrazující pasivní konzumaci mediálního obsahu,[4] informatizace zasahující sektor vzdělávání[5] a dokonce i změn v právní praxi. Dochází tedy ke změnám ve všech oblastech lidské činnosti, ve struktuře společnosti samé, a ve způsobu, jakým komunikuje – mluvíme o tzv. informační společnosti.

Prvním krokem k tak masivnímu nárůstu rychlosti výměny informací byla bezpochyby digitalizace. Digitalizace umožnila uvést informaci do zcela univerzálně duplikovatelné a šiřitelné formy. Druhým krokem je pak neustálé zvyšování výpočetní kapacity za současného snižování ceny.[6] Rychlost šíření informací se tedy zvyšuje a zároveň se nástroje pro zrychlenou výměnu stávají univerzálně dostupnými napříč všemi příjmovými skupinami.

Proliferace informačních technologií je racionálním evolučním krokem v životě společnosti, která zcela přirozeně inklinuje k maximalizaci míry organizace, čehož dosahuje právě vyšší mírou informovanosti. Klíčové je vyvarovat se při popisu informační společnosti tvrzení, že změna paradigmatu byla způsobena samotným užíváním informací. Všechny předchozí stupně ve vývoji společnosti informace vždy využívaly. Změna paradigmatu souvisí se způsobem (s kvalitou) využívání těchto informací. Jedná se o uvědomělé využívání informací při organizaci společnosti – o vědomou podporu (institucionalizovanou či nikoli) využívání moderních technologií při výměně informací. Podporu ze strany vlád,[7] mezinárodních organizací či občanských iniciativ. Samotný fakt využívání informací při organizaci je přirozený pro každou společnost. Informační společnost stojí na bezprecedentní rychlosti šíření informací a na vysoké míře informovanosti.

Z hlediska vývoje konkrétních aspektů společnosti můžeme mluvit o ekonomickém, pracovním, teritoriálním či kulturním pohledu na informační společnost a také o změně v celkovém vnímání prostoru.[8] Tímto rozdělením můžeme konkrétně zkoumat, co všechno se ve společnosti změnilo a jakým způsobem. V nepo-

1 Více viz WIENER, Norbert. *Kybernetika a společnost.* Praha: Československá akademie věd, 1963. 216 s.

2 KLIMEK, Libor. *Combating Attacks Against Information Systems: EU Legislation and its Development. Masaryk University Journal of Law and Technology.* 2012, roč. 6, č. 1, s. 87-100. ISSN 1802-5943. S. 87.

3 BASTL, Martin. *Kybernetický terorismus: studia nekonvenčních metod boje v kontextu soudobého válečnictví.* Brno, 2007. 153 s. Disertační práce, Masarykova univerzita, Fakulta sociálních studií. S. 14 a násl.

4 MCLUHAN, Marshall. Understanding media: the extensions of man. Cambridge: MIT Press, 1995. 365 s. ISBN 0262631598. S. 30 a násl.

5 POOLE, John Bernard et al. *Education for an Information Age: Teaching in the Computerized Classroom.* 7th Edition [online]. 2009 [cit. 8. 11. 2012]. Dostupné z: http://www.pitt.edu/~poole/InfoAge7frame.html.

6 Jedná se o tzv. Mooreův zákon.
ZLATUŠKA, Jiří. *Informační společnost. Zpravodaj ÚVT MU* [online]. 1998, roč. 8, č. 4, s. 1-6 [cit. 9. 11 .2012]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/articles/122.html.

7 V ČR spadá agenda informační společnosti do dikce Rady vlády pro konkurenceschopnost a informační společnost, která byla ustavena na základě usnesení vlády č. 293 z 28. 3. 2007.

8 WEBSTER, Frank. *Theories of the Information Society. Third edition.* London: Routledge, 2006. 317 s. ISBN 0-415-40633-1. S. 8-9.

slední řadě můžeme pojmenovat i dopady na příslušné aspekty života jednotlivce a života samotné společnosti.

Technologicky se jedná z hlediska kvantitativního o společnost, která má rozsáhlý přístup k informačním a komunikačním technologiím. Z hlediska kvalitativního pak o celospolečensky větší míru organizovanosti díky využití těchto technologií.[9] Tento pohled na informační společnost je přímo možné potvrdit při pohledu na statistiky – v provozu je po světě zhruba 1,6 miliardy počítačů[10] a téměř 7 miliard mobilních telefonů.[11] Tyto počty pak nutně mění způsoby komunikace a samozřejmě vyvolávají celospolečenskou, někdy až překvapivou, závislost na fungování těchto systémů.[12] Ze strany vyspělých států a jejich obyvatel je spatřována jistá nutnost umožnit přístup k těmto technologiím i rozvojovým státům a jejich obyvatelům, což se promítá do podpory konkrétních projektů.[13] Závislost na technologiích při sociální a obchodní interakci má i konkrétní právní konsekvence. Jakmile virtualizace vztahu dosáhne určité míry, je nutné upravit právní režim za účelem zachování efektivní právní ochrany.[14]

Podle některých teorií je možné mluvit o informační společnosti ve chvíli, kdy větší část ekonomické produktivity připadne informačním aktivitám (ve srovnání s tradičními odvětvími).[15] V souvislosti s ekonomickými změnami se také mluví o vzniku post-industriální společnosti, která reflektuje posun těžiště ekonomické aktivity do samostatného odvětví produkce a zpracování informací. Podle některých dalších autorů naopak není zásadním znakem informační společnosti nárůst odděleného sektoru zaměřeného výhradně na zpracovávání informací. Rozdíl spatřují hlavně v nárůstu produkce a zpracování informací ve všech sektorech, včetně tradičních, jako je zemědělství či průmysl.[16] I vzhledem ke kritickým připomínkám směrem k tzv. informační ekonomice se jeví tento přístup jako opatrnější a zároveň i věcně správnější. Naše společnost se zatím, přes veškerou informatizaci a veškeré výhody z ní plynoucí, nedokázala oprostit od závislosti na průmyslové produkci. Ani prudce rostoucí sektor služeb nedokáže plně nahradit stagnující průmysl.[17]

Zásadní roli hraje informatizace na ekonomickém poli při alokaci prostředků a zdrojů. S větší mírou informovanosti je možné zasadit probíhající transakci do rámce tržního prostředí porovnáním např. s plněními poskytnutými u jiných transakcí stejného typu. Důsledkem je pak jednodušší dosažení nejvýhodnější nabídky. Díky informačním technologiím je možné lehce překonat geografickou či kulturní vzdálenost při hledání výhodnějšího obchodu.[18] Převažující názor na ekonomickou roli informačních technologií v rámci informační společnosti by se tedy dal shrnout tak, že virtuálno nenahrazuje skutečnost, ale zvyšuje možnost jejího uskutečnění.[19] Zároveň pak informační technologie představují tzv. univerzálně generickou inovaci. Tato inovace definuje nové paradigma, v rámci kterého vzniká nový technologický režim ovlivňující metody ve všech hospodářských odvětvích a sektorech.[20]

Z hlediska pracovního trhu je změna spatřována v navýšení podílu zaměstnanců, kteří se zaměřují na zpracování informací,[21] a také v nárůstu poptávky po specifickém vzdělání či specifických schopnostech. Existující profese se nejenom přizpůsobují svojí pracovní náplní tomuto vývoji, ale vznikají i profese zcela nové. Tyto jsou spojené s vysoce specializovanými úkony v rámci produkce a zpracování informací.[22] V souvislosti se změnou v zaměření tradičních profesí je možné mluvit i o profesi právní. Zatímco na straně právníků bylo v minulosti právo informačních a komunikačních technologií zpochybňováno jako „koňské právo“,[23] dnes se již stává běžnou součástí právního vzdělání i právní praxe. Mění se požadavky soukromého sektoru z hlediska znalostí, které musí právník zvládat (právní aspekty softwaru atp.). Také se rozšiřuje využívání nástrojů umožňujících efektivnější práci a stává se samozřejmostí i pro konzervativnější část odborné právnické veřejnosti.[24]

9 Tamtéž, s. 9-12.

10 *PCs In-Use Worldwide reaches over 1.6BUnits in 2011. USA has nearly 311M PCs In-Use* [online]. ETForecasts, 2012 [cit. 8. 11. 2012]. Dostupné z: http://www.etforecasts.com/pr/pr020112.htm.

11 *Key 2006-2013 ICT data* [online]. International Telecommunication Union, 2013 [cit. 16. 10. 2013]. Dostupné z: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

12 Viz např. COPPING, Jasper. *Warning over decline in map skills as ramblers rely on sat navs.* Telegraph.co.uk [online]. 2012 [cit. 8. 11. 2012]. Dostupné z: http://www.telegraph.co.uk/earth/countryside/9090729/Warning-over-decline-in-map-skills-as-ramblers-rely-on-sat-navs.html.

13 Např. projekt One Laptop per Kid, jehož domovská stránka se nachází na http://one.laptop.org/.

14 POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3. S. 275.

15 WEBSTER 2006 op. cit., s. 12.

16 DIJK, Jan van. *The Network Society*. 3rd edition. Thousand Oaks: Sage Publications, 2012. 326 s. ISBN 9781446248959. S. 19.

17 Jeden z vedoucích heterodexních ekonomů Ha-Joon Chang dokonce tvrdí, že nahrazení průmyslu sektorem služeb je principiálně nemožné. Vzhledem k omezenému exportu služeb může mít krize domácí poptávky na takto strukturovanou ekonomiku katastrofální následky. Internetový boom také označuje za hype, protože má podle něj mnohem menší dopad na rychlost komunikace ve vztahu k faxu, než měl telegraf ve vztahu k poště.
CHANG, Ha-Joon. *23 Things They Don't Tell You About Capitalism.* London: Allen Lane, 2011. 286 s. ISBN 9781846143281.
Viz také SALOMON, Jean-Jacques. *Technologický úděl.* Praha: Filosofia, 1997. 287 s. ISBN 8070070978. S. 106.

18 Přímo v českých podmínkách můžeme v této souvislosti teoreticky hovořit o projektu elektronické aukce léků. Tyto aukce mají snižovat cenu léků pro české zdravotnictví za pomoci kumulace objednávek a tím pádem zvýšení tržního potenciálu nakupujících zdravotnických zařízení.

19 Lévy mluví o nižší časové i ekonomické náročnosti vyhledání starého přítele při použití internetu. Tento závěr je použitelný i na vyhledávání nových příležitostí v rámci tržní ekonomiky.
LÉVY, Pierre. *Kyberkultura: zpráva pro Radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace“.* Praha: Karolinum, 2000. 229 s. ISBN 8024601095. S. 78-79.

20 Jedná se o Schumpeterův pojmový aparát. SALOMON 1997 op. cit., s. 106.

21 WEBSTER 2006 op. cit, s. 14.

22 Úzce souvisí i s taylorismem a vědeckou organizací práce. SALOMON 1997 op. cit., s. 165-184.

23 EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse* [online]. Chicago: University of Chicago Legal Forum, 1996 [cit. 2. 11. 2012]. 5 s. Dostupné z: http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf.

24 Jedná se zde zejména o různé právní informační systémy, které se snaží přizpůsobovat poptávce. Na tento vývoj reaguje i česká akademická scéna, která systémy již i kriticky posuzuje (namísto dosavadního pouhého popisu jejich funkčnosti). Poměrně zajímavá je v tomto ohledu diskuze na webu Jiné Právo s příspěvky např. od Zdeňka Kuhna či Jaromíra Šavelky.

Informační společnost je dále možné popsat i změnami, které přinesla z hlediska celkového pojetí prostoru. Došlo k delokalizaci společenských vztahů při zachování jejich náplně a podstaty.[25] Kromě možnosti popsání informační společnosti tímto znakem se také jedná o základní problém práva v rámci takto zformované společnosti. Absence fyzické lokalizace způsobuje teoretické i praktické problémy při uplatňování státní moci.[26] Zároveň ale snižuje dobu šíření informace na absolutní minimum, protože geografické hranice nadále nehrají takovou roli jako dřív.[27]

S pojetím prostoru souvisí i samotné pojetí komunikace a jejích výstupů. V rámci informační společnosti je možné pozorovat virtualizaci společenského života do bezprecedentní míry. Faktický vliv virtualizace je vzhledem k lidské psychologii poměrně zásadní. Z výzkumů plyne, že s rostoucí geografickou vzdáleností je mnohem jednodušší způsobit jiné lidské bytosti újmu.[28] Informační společnost upřela roli geografické vzdálenosti a nahradila ji jinou formou odtělesnění, kterou je právě virtualizace. S vývojem rychlosti komunikace zmizela její bezprostřednost, schopnost empatie k citům konverzačních protějšků,[29] zrelativizovalo se dodržování závazků i schopnost cenit si vlastních osobních informací.[30]

Kulturní posun je pak spatřován ve stále rostoucí roli kvalitního marketingu oproti kvalitním službám,[31] v umocňující se roli médií při definici kultury[32] a v důrazu na kvantitu oproti kvalitě.[33] Podstatné jsou také změny v kulturní rozmanitosti – na jednu stranu se mainstreamová kultura standardizuje na globální úrovni, na druhou stranu se pak odchylky od mainstreamu mají možnost globálně sdružovat a vyměňovat si své kulturní zkušenosti.[34] Jedním ze zmiňovaných kulturních posunů je také důležitější role vědy,[35] která při sílící racionalizaci společnosti do určité míry fakticky nahrazuje náboženství.[36]

Výše popsané změny v konkrétních aspektech společnosti nejsou zcela vyčerpávající a proto se pro účely univerzálního popsání (zvláště vhodného vzhledem k univerzalitě práva) zavádějí nejobecnější perspektivy – kvalitativní a kvantitativní.[37] Kvalitativně je informační společnost vymezena zaměřením se na kvalitu komunikovaných informací[38] a kvantitativně pak mírou vzájemného propojení jednotlivých subjektů a jejich možnosti svobodně komunikovat informace.[39] Podle některých autorů je dokonce možné po překročení určité kvantitativní úrovně informační společnosti očekávat přirozenou seberegulaci bez nutnosti autority, spontánní řád.[40]

Vědomý rozvoj informační společnosti probíhal v České republice pochopitelně s určitým zpožděním oproti západoevropským zemím. Česká republika se nicméně otázce věnovala již před svým vstupem do EU v roce 2004. K 1.1.2003 tak bylo zákonem č. 517/2002 Sb.[41] zřízeno Ministerstvo informatiky České republiky jako *„ústřední orgán státní správy pro informační a komunikační technologie, pro telekomunikaci a poštovní služby.“*[42] Ministerstvo informatiky bylo celoevropsky poměrně unikátním orgánem, který se ale ve své činnosti často omezoval pouze na překládání úpravy ve členských státech EU a nepřinášel žádnou invenční činnost. Ministerstvo informatiky zaniklo k 1. 6. 2007 zákonem

Viz KÜHN, Zdeněk. *Jak zlepšit české právní informační systémy?* Jiné Právo [online]. 2008 [cit. 7. 9. 2012]. Dostupné z: http://jinepravo.blogspot.cz/2008/02/jak-zlepit-esk-prvn-informan-systmy.html.

Viz ŠAVELKA, Jaromír. *Jak zlepšit zpřístupňování judikatury?* Jiné Právo [online]. 2012 [cit. 7. 9. 2012]. Dostupné z: http://jinepravo.blogspot.cz/2012/04/jaromir-savelka-jak-zlepsit.html.

25 POLČÁK 2012 op. cit., s. 276.

26 Což samozřejmě může být i výhoda zcela legitimní. Na otázku, zda-li je důležitější mít chleba nebo přístup k internetu odpověděl jeden lidskoprávní aktivista: „Bez přístupu k internetu nemůžeme světu říct, kdo nám krade chleba.“ KETTEMANN, Matthias. *UN Human Rights Council Confirms that Human Rights Apply to the Internet.* EJIL: Talk! [online]. 2012 [cit. 25. 7. 2012]. Dostupné z: http://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/.

Z důvodu medializace je poměrně slavným případem také zatčení amerického studenta žurnalistiky Jamese Bucka v Egyptě. Ten informoval o svém zatčení pomocí Twitteru, v reakci na ten mu pak jeho přátelé a univerzita téměř okamžitě zajistili právní pomoc. Z vězení byl propuštěn hned druhý den, zatímco jeho kolega pobyl ve vězení tři měsíce.

Student ‚Twitters' his way out of Egyptian jail. CNN.com [online]. 2008 [cit. 4. 11. 2012]. Dostupné z: http://articles.cnn.com/2008-04-25/tech/twitter.buck_1_cell-phone-blog-anti-government-protest?_s=PM:TECH.

Případ zmiňuje i COMM, Joel; ROBBINS, Anthony; BURGE, Ken. *Twitter Power.* Hoboken: John Wiley & Sons, 2009. 248 s. ISBN 047058429.

27 Nic samozřejmě není ideální, což se týká i odstranění geografických limitů pro šíření informací. Na internetu např. existuje nástroj, který slouží k testování dostupnosti serverů v Číně (kvůli existenci tzv. Čínského firewallu). Dostupné na http://www.greatfirewallofchina.org/ [cit. 4. 11. 2012].

28 I když si člověk uvědomuje následky svého konání, umožňuje mu geografická vzdálenost dehumanizovat protivníka. O fenoménu poměrně vyčerpávajícím způsobem z vojenského pohledu pojednává GROSSMANN, D. *On Killing: The Psychological Cost of Learning to Kill in War and Society.* Boston: Little Brown, 1995. 367 s. ISBN 0316330000.

29 Z toho plyne i rozšíření tzv. flame war a trollů v různých internetových diskuzích. O tomto fenoménu se zmiňuje i Pierre Lévy. LÉVY 2000 op. cit., s. 85-88.

30 SULER, John. *The Online Disinhibition Effect* [online]. 2004 [cit. 12. 1. 2013]. Dostupné z: http://users.rider.edu/~suler/psycyber/disinhibit.html.

31 POLČÁK 2012 op. cit., s. 277.

32 DIJK 2012 op. cit., s. 19.

33 Tamtéž, s. 199-204 a 208-209.

34 Tamtéž, s. 191-192.

35 Tamtéž, s. 19.

36 Salomon popisuje snahu odborníků bránit svůj obor proti zasahování zvenčí (tedy proti zasahování laiků) při posuzování rizik technologického vývoje. SALOMON 1997 op. cit., s. 37-51.

37 WEBSTER 2006 op. cit, s. 21-24.

38 Tedy jejich způsobilosti ke snižování společenské entropie.

39 POLČÁK 2012 op. cit., s. 277-279 a s. 23 a násl.

40 Tomuto tématu se poměrně intenzivně věnují přírodní vědy, viz KAUFFMAN, Stuart A. *At home in the universe: the search for laws of self-organization and complexity.* New York: Oxford Unviersity Press, 1995. 321 s. ISBN 0195111303.

Hartzog používá pojem „*order without orderer*.“ HARTZOG, Paul B. *Panarchy: Governance in the Network Age.* [online]. Salt Lake City, 2005 [cit. 10. 11. 2012]. Diplomová práce. University of Utah. Dostupné z: http://www.academia.edu/210378/Panarchy_Governance_in_the_Network_Age. S.11-12.

Jedná se také o jednu z premis Deklarace nezávislosti kyberprostoru. BARLOW, John Perry. *Declaration of Independence of Cyberspace* [online]. Davos: 1996 [cit. 10. 11. 2012]. Dostupné z: https://projects.eff.org/~barlow/Declaration-Final.html.

Za odpůrce této teze lze v českém prostředí označit Polčáka, který možný návrat Zlatého věku odmítá na základě empirických důkazů o nárůstu výskytu patologických jevů v informačních sítích. POLČÁK 2012 op. cit., s. 101.

41 Zákon č. 517/2002 Sb., kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. Atlas Consulting [cit. 26. 1. 2013].

42 Ustanovení §2, odst. 7 zákona č. 517/2002 Sb.

č. 110/2007 Sb.[43] Jeho kompetence pak byly rozmělněny mezi Ministerstvo vnitra, Ministerstvo průmyslu a obchodu a Ministerstvo místního rozvoje. Ve stejné době Vláda ČR rozhodla o zřízení Rady vlády pro informační společnost, která po změnách funguje dodnes jako Rada vlády pro konkurenceschopnost a informační společnost.[44] Tato rada pak plní koordinační úlohu zrušeného Ministerstva informatiky a poskytuje Vládě ČR vědomostní základnu pro rozhodnutí o koncepčních otázkách souvisejících s rozvojem informační společnosti v ČR.

Přístup České republiky k informační společnosti je dlouhodobě kritizován pro svoji nekoncepčnost a upřednostnění partikulárních velkých projektů při neexistující technické standardizaci.[45] Proto se orgán na vládní úrovni jeví obzvláště vhodným jako shromaždiště rezortních připomínek. Ideálně by Rada měla přispívat k široké diskuzi a analýze potřeb jednotlivých odvětví státní správy a zároveň navrhovat komplexní technická i legislativní řešení pro odstranění nedostatků. V současné době se tak bohužel neděje.

Pokud chceme hodnotit penetraci informačních technologií v české společnosti, můžeme využít statistik poskytovaných ČSÚ. V roce 2012 bylo 67,3% českých domácností vybaveno počítačem a 65,4 % českých domácností bylo vybaveno připojením k internetu.[46] Jedná se tak o značný nárůst v relativně krátké době, protože v roce 2005 disponovalo připojením k internetu jen 19,1 % českých domácností.[47] V kombinaci s různými službami umožňujícími dálkový přístup, postupným rozvojem eJustice a eGovernmentu je tedy možné konstatovat, že informační technologie jsou v české společnosti široce zastoupené a podíl domácností i podniků, které je využívají, se zvyšuje. To vše se pak děje při výše zmíněné nekoncepčnosti přístupu „shora", resp. absenci koncepce navzdory.[48]

1.2 Informační sebeurčení

V předchozí kapitole byla, pomocí popisu společenských změn, schematicky nadefinována informační společnost. Z kontextu takto definované společnosti pak vychází informační sebeurčení jednotlivce – tedy hodnota, která má být předmětem ochrany ze strany kybernetické bezpečnosti. Právo na informační sebeurčení existuje v současné době v kontextu informační společnosti jako její integrální součást, na kterou je nutné klást značný důraz. Jedná se o katalog distributivních práv, bez kterého by kybernetická bezpečnost (jako nedistributivní informační právo) zcela postrádala smysl a zároveň by nemohla být v žádném případě legitimní.

Pojem informačního sebeurčení se objevil v Německu v první polovině osmdesátých let. Spolkový ústavní soud tehdy zohlednil vývoj, kdy se zásahy do informačního soukromí jednotlivců začaly objevovat jako systémový fenomén. Vznikla tak potřeba se vůči tomuto fenoménu vymezit. V rozhodnutí se uvádí: *„Ochrana základních práv zahrnuje též způsobilost člověka určit v zásadě dostupnost a užití jeho/jejích osobních údajů."*[49] Pod rozsah informačního sebeurčení je v současné době možné zahrnout nejenom pasivní ochranu vlastních soukromých údajů, ale i aktivní práva na získávání, zpracování a komunikaci informací.

Je důležité připomenout, že stejně jako není novinkou související s rozvojem informační společnosti využívání informací při organizaci, není novinkou ani koncept informačního sebeurčení. Kvalitativně rozvoj informační společnosti nepřináší v tomto ohledu nic nového. Na druhou stranu ale, jak již bylo zmíněno výše, roste uvědomění si hodnoty a role informací v životě společnosti i jednotlivce. S tím pak roste i společenská hodnota a úloha informačního sebeurčení.

Zásadním problémem pojmu informačního sebeurčení se může zdát jeho relativní neurčitost. Jedná se o stále se rozvíjející komplex distributivních informačních práv, jejichž konkrétní obsah se mění v závislosti na používaných technologiích. S rozvojem nových forem komunikace se rozvíjí i formy omezování informačních práv jednotlivce.[50] V současné době je možné za součást informačního sebeurčení označit následující distributivní informační práva:

- svobodu projevu a vědeckého bádání
- ochranu soukromí, osobnosti a práva na aktivní soukromý život
- právo na vzdělání
- ochranu osobních údajů
- právo na informace veřejného sektoru.[51]

Důležitost pojímání informačního sebeurčení jako katalogu distributivních práv tkví v komplexitě tohoto pojetí.[52] Ochrana soukromí nebo právo na informace veřejného sektoru jsou samostatně stojící vnímána jako důležitá informační práva. Až zdůrazněním společné

43 Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů. In: *CODEXIS* [právní informační systém]. Atlas Consulting [cit. 26. 1. 2013].

44 Webová stránka se nachází na http://www.vlada.cz/cz/ppov/rvis/rada-vlady-pro-konkurenceschopnost-a-informacni-spolecnost-73372/ [cit. 16. 3. 2013].

45 POLČÁK 2012 op. cit., s. 297-298.

46 *Vybavenost domácností osobních počítačem a internetem podle typu domácnosti, velikosti obce příjmové skupiny krajů* [online]. Český statistický úřad [cit. 16. 10. 2013]. Dostupné z: http://vdb.czso.cz/vdbvo/tabparam.jsp?childsel0=1&cislotab=ICT0070PU_KR&kapitola_id=420&voa=tabulka&go_zobraz=1&childsel0=1.

47 *Domácnosti s připojením k internetu* [online]. Český statistický úřad, 2012 [cit. 26. 1. 2013]. Dostupné z: http://notes.czso.cz/csu/redakce.nsf/i/informacni_technologie_pm.

48 Vývoj navzdory absenci centrální koncepce lze také použít jako důkaz o přirozenosti tohoto vývoje.

49 Nález Spolkového ústavního soudu ze dne 15.12.1983, č.j. BverfGE 65, 1 [cit. 16. 10. 2013]. Dostupné z: http://www.servat.unibe.ch/dfr/bv065001.html. Překlad dle POLČÁK 2012 op. cit., s. 325.

50 Např. dokud nebyl internet masově rozšířen, nemělo smysl uvažovat o přístupu k němu jako o integrální součásti informačního sebeurčení. Stejná je i situace biometrických údajů, kdy nebylo nutné řešit limity jejich použití, dokud se nestaly dostupnou technologií.

51 POLČÁK 2012 op. cit., s. 326-327.
K poslednímu zmiňovanému distributivnímu právu je možné např. poukázat na projekt Otevřená data (domovská stránka na http://www.otevrenadata.cz/), diskuzi o rozšíření působnosti NKÚ, diskuzi o novelizaci zákona č. 106/99 Sb. atd.

52 Více COVENEY, Peter; HIGHFIELD, Roger. *Mezi chaosem a řádem.* Praha: Mladá fronta, 2003. 428 s. ISBN 8020409890.

funkce a společného původu je jim ale přiznána, na úrovni komplexního pojmu informačního sebeurčení, důležitost mnohem větší. Komplexní efekt tak ústí ve vyšší intenzitu závažnosti informačního sebeurčení v porovnání se závažností jeho jednotlivých komponent.

Informační sebeurčení má přímou vazbu na samotnou informační podstatu života.[53] Vzhledem k rychlosti technologického vývoje na poli komunikací je nemožné přesně popsat obsah (strukturálně i pojmově) informačního sebeurčení v daném okamžiku. Pojetí informačního sebeurčení se také může lišit (a liší) v kontextu jednotlivých právních tradic – vzhledem k euroatlantické orientaci platného práva na člověka se dnes pod informační sebeurčení neřadí korporátní či státní informační práva.[54]

V minulosti se pojem informačního sebeurčení již několikrát diskutoval v české soudní praxi i mimo kontext informačních technologií, zejména pak v otázce ochrany osobnosti. Ústavní soud např. konstatoval, že základní právo na čest je uplatňováno ve více sférách. V rámci sféry první, soukromé, je každý nadán absolutním informačním sebeurčením. Sám si tedy může rozhodnout, co z tohoto segmentu uvolní, a co naopak nikoli. Zvenčí pak do této sféry nelze vstupovat. Ve sféře druhé, společenské, může existovat určitý veřejný zájem.[55] Nález Ústavního soudu sp. zn. I. ÚS 453/2003 ze dne 11. 11. 2005[56] vysvětluje, že *„jednotlivec žije ve společenství a vstupuje s ostatními jeho členy do komunikace a skrze své chování, ba dokonce skrze své samotné bytí, ovlivňuje ostatní členy společenství.“* Téměř totožnou formulaci pak obsahuje i Nález Ústavního soudu IV. ÚS 23/2005 ze dne 17. 7. 2007.[57] Z toho důvodu zde již tedy neplatí absolutní informační sebeurčení a veřejná moc může proporcionálně zasahovat v zájmu společenství.

Vlastní čest člověka tedy musí být chápána ve dvou úrovních, kdy výhradní dispozice se týká pouze úrovně první, do které neoprávněně zasahují i pravdivé výroky. Dispozice se ale vztahuje i k možnosti jednotlivce se samotným chováním z ochrany vyloučit, jak ostatně připouštělo již socialistické soudnictví, kdy soud např. dovodil, že *„[by bolo] treba brať do úvahy, že občan (občania) sám (sami) svojím chovaním určitú skutočnosť z chránenej sféry intímneho života vylúčil (vylúčili) […], takže se zbavil (zbavili) možnosti úspešne žalovať […].“*[58] Tento trend je ostatně možné pozorovat i v novější odborné literatuře.[59]

Jak již bylo v tomto textu zmíněno, vývoj v České republice je znatelně pomalejší než v západoevropských zemích. Koncept informačního sebeurčení v kontextu informačních technologií tak začíná přitahovat pozornost až v posledních několika letech. Získává na důležitosti v soudních rozhodnutích nejvyšších soudů a v akademické sféře, a to hlavně v kontextu ochrany soukromí. Za svého způsobu revoluci se dá označit nález Ústavního soudu ČR I. ÚS 22/10 ze dne 7. 4. 2010,[60] kdy soud přiznal ochranu individuální internetové konektivitě. Přístup k internetu vyložil jako extenzi práva na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi, která je integrální součástí respektování soukromého života.[61] V disentním stanovisku soudkyně Ivany Janů je sice poukázáno na některé problémové aspekty zmíněného rozhodnutí,[62] celková logika však reflektuje současnou úlohu internetového připojení pro soukromý život jednotlivce i současný přístup k rozvoji informační společnosti.[63] Tento nález je tak velice pří-

53 WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s.

54 Srovnej s Freedmanem, který komentuje snahu o ochranu tajných státních dokumentů v kauze Wikileaks na základě autorských práv a nikoli na úrovni státních informačních práv.

FREEDMAN, James. *Protecting State Secrets as Intellectual Property: A Strategy for Prosecuting Wikileaks. Stanford Journal of International Law.* [online]. 2012, roč. 48, č. 1, s. 185-208 [cit. 17. 5. 2012]. ISSN 0731-5082. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042692.

55 Nález Ústavního soudu ČR ze dne 15. 5. 2012, sp. zn. II. ÚS 171/12. In: NALUS [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

56 Nález Ústavního soudu ČR ze dne 11. 11. 2005, sp. zn. I. ÚS 453/2003. In: NALUS [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

57 Nález Ústavního soudu ČR ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/2006. In: NALUS [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

58 POKORNÝ, Milan (red.). *Nejvyšší soud o občanském soudním řízení v některých věcech pracovněprávních, občanskoprávních a rodinněprávních: sborník stanovisek, závěrů, rozborů a zhodnocení soudní praxe, zpráv o rozhodování soudů a soudních rozhodnutí Nejvyššího soudu. 1964–1969.* Praha: SEVT, 1980. 439 s. S. 196.

59 *„Pokud však pacient sám zveřejní v tisku či jiném hromadném sdělovacím prostředku svůj vlastní zdravotní případ s uvedením skutečností, podléhajících povinnosti mlčenlivosti ze strany lékaře […] nemusí povinnost mlčenlivosti dodržovat ani lékař.“*

KNAP, Karel et al.. *Ochrana osobnosti podle občanského práva.* 4. podstatně přepracované a doplněné vydání. Praha: LINDE, 2004. 435 s. ISBN 8072014846. S. 224.

60 Nález Ústavního soudu ČR ze dne 7. 4. 2010, sp. zn. I. ÚS 22/10. In: NALUS [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

61 Nález Ústavního soudu ČR ze dne 1. 3. 2000, sp. zn. IV. ÚS 517/99. In: NALUS [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

62 Ivana Janů mj. podotýká, že *„[p]odle tohoto způsobu uvažování by každé rozhodnutí soudu, jímž se zasáhne majetková sféra osoby natolik, že si nebude moci dovolit platit poplatky za kabelovou televizi a internet, mělo být hodnoceno jako porušení práva na soukromý a rodinný život.“* Zjevně tak kritizuje příliš extenzivní roli, kterou soud přisoudil při rozhodování o bezplatné obhajobě právu na soukromý a rodinný život. Problematičnost předmětného nálezu zmiňuje stručně i Polčák nebo Kmec.

Viz POLČÁK 2012 op. cit., s. 326.

Viz KMEC, Jiří. Ústavní soudci, mluvíte spolu? Jiné Právo [online]. 2010 [cit. 24. 1. 2013]. Dostupné z: http://jinepravo.blogspot.cz/2010/05/ustavni-soudci--mluvite-spolu.html.

63 Za všechny příklady tendencí na poli individuálního připojení k internetu lze jmenovat *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* z pera Franka La Rue. Frank La Rue mimo jiné zmiňuje, že „odstřižení“ od internetu je v hrubém nepoměru k jakémukoli porušení práv duševního vlastnictví.

LA RUE, Frank. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* [online]. UN General Assembly, 2011 [cit. 27. 1. 2013]. Dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Tím naráží i na Francii, kde funguje tzv. třikrát a dost. K tématu blíže HABER, Eldar. *The French Revolution 2.0: Copyright and the Three Strikes Policy. Harvard Journal of Sports and Entertainment Law* [online]. 2011, roč. 2, č. 2, s. 298-339 [cit. 20. 2. 2012]. ISSN 2153-1323. Dostupné z: http://heinonline.org. Velice zajímavým je také rozhodnutí soudu v Karlsruhe ze dne 24. 1. 2013, kdy soud přiznal náhradu za nemožnost používat internet. Viz *Tisková zpráva č. 14/13 ze dne 24. 1. 2013 k rozhodnutí III ZR 98/12* [online]. Karlsruhe: 2013 [cit. 28. 1. 2013]. Dostupné z:http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&-nr=62927&linked=pm.

nosným a jeho důležitost byla reflektována i v rámci prací směřujících k přípravě české legislativy v oblasti kybernetické bezpečnosti.[64] Důvodová zpráva zákona o kybernetické bezpečnosti zmiňuje dělení práv spadajících pod komplexní pojem informačního sebeurčení na pasivní (ochrana soukromí atp.) a aktivní (přístup ke službám informační společnosti) a vychází z premisy, že bez aktivní složky není možný plnohodnotný soukromý ani společenský život.[65] Celá připravovaná legislativa se tak hlásí k minimalistickému přístupu ke kybernetické bezpečnosti z hlediska povinností ukládaných soukromoprávním subjektům.

Výše zmíněný nález pak zdaleka nepředstavuje exces v rozhodovací praxi, ale spíše vyústění současných trendů. Koncept informačního sebeurčení je v judikatuře Ústavního soudu aktuální i ve společensky a mediálně nejsledovanějších věcech. Objevil se v Nálezu Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011,[66] který bude zmíněn dále v textu v kontextu proporcionality.[67] Důležitost informačního sebeurčení byla zohledněna i ve věci přístupu orgánů činných v trestním řízení k údajům o telekomunikačním provozu podle §88a zákona č. 141/1961 Sb.[68] Ústavní soud ve svém Nálezu ve věci Pl. ÚS 24/11 ze dne 20. 12. 2011[69] dovodil, že přístup orgánů činných v trestním řízení k údajům o telekomunikačním provozu bez souhlasu uživatele představuje závažnou invazi do sféry informačního sebeurčení. I na základě toho konstatoval protiústavnost výše zmíněného ustanovení §88a. Informační sebeurčení hrálo důležitou úlohu i při rozhodování Ústavního soudu ve věci zrušení zákona 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. V rámci Nálezu ve věci Pl. ÚS 1/12 ze dne 27. 11. 2012[70] soud konstatoval, že předmětná úprava není přiměřená účelu použití osobních údajů, čímž je zasaženo do informačního sebeurčení jednotlivců, na které ustanovení dopadá.

V rámci diskuzí o informačním sebeurčení je v poslední době věnována pozornost také nastavení limitů svobody projevu v prostředí počítačových sítí. Jedná se hlavně o aktuální formu protestu v prostředí internetu, tedy DDoS[71] útoky,[72] jejichž povaha je problematická.[73] Někteří autoři např. zmiňují „digital sit-in" v kontextu zablokování digitálního provozu jako ekvivalent protestního zablokování komunikace v aktuálním světě za účelem upozornění na určitý problém.[74] Narušování digitálního provozu může být tedy vnímáno jako extenze občanské neposlušnosti do kyberprostoru. Jedním ze znaků občanské neposlušnosti je ilegalita takového počínání.[75] Snahy o legalizaci DDoS útoků[76] pak mohou směřovat nikoli k cestě DDoS útoků jako projevu občanské neposlušnosti, ale přímo k dočasnému narušení digitální komunikace jako extenzi práva na svobodu projevu.

Zásadním a hojně diskutovaným aspektem informačního sebeurčení je v kontextu s výše zmíněnou digitalizací a univerzální přenositelností dat i ochrana osobních údajů a dat. Rozvoj informačních technologií při současném nedodržování bezpečnostních standardů[77] (či jejich časté úplné absenci) umožnil opakované úniky osobních dat z databází jednotlivých firem, ať již za účelem zisku či určité formy protestu.[78] V USA je problematika ochrany osobních údajů rozsáhle diskutována i v kontextu Čtvrtého dodatku[79] či v kontextu tzv. práva „to be let alone."[80]

64 *Důvodová zpráva k zákonu o kybernetické bezpečnosti* [online]. 2013 [cit. 15. 10. 2013]. Dostupné z: http://www.govcert.cz/download/nodeid-1855/.

65 Důvodová zpráva 2013 op. cit., s. 65.

66 Nález Ústavního soudu ČR ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

67 Jednalo se o uchovávání provozních a lokalizačních údajů.

68 Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění k 1. 2. 2011. In: Úplné znění č. 825. Sagit.

69 Nález Ústavního soudu ČR ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/11. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

70 Nález Ústavního soudu ČR ze dne 27. 11. 2012, sp. zn. Pl. ÚS 1/12. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

71 Distributive Denial of Service.

72 Zejména se jedná o hnutí Anonymous, potažmo českou skupinu Czechurity. K protestnímu charakteru jejich činnosti lze najít informace např. v rozhovoru s jedním ze členů.
Nejde nám o peníze, ale o názor, tvrdí hackeři. Ekonom. 2013, č. 4, s. 8-9. ISSN 1213-7693.

73 USA již má s případy stíhání za DDoS jistou praxi. Za high-profile je např. označován případ, který je veden v Kalifornii pod číslem CR 11-00471 DLJ. V něm je momentálně stíháno 15 hackerů, kteří údajně stáli za DDoS útoky na PayPal.
V ČR je situace problematičtější, případný DDoS útok by dle autorova názoru nemohl spadat ani pod skutkovou podstatu ustanovení §230, odst. 3, písm. b) Trestního zákoníku.

74 ARQUILLA, John; RONFELDT, David (eds.). *Networks and Netwars: Future of Terror, Crime and Militancy.* Santa Monica: RAND Corporation, 2001. 380 s. ISBN 0-8330-3030-2. S. 265-268.

75 MCLAURIN, Joshua. *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks. Yale Law & Policy Review* [online]. 2011, roč. 30, č. 1, s. 211-254 [16. 8. 2012]. ISSN 0740-8048. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1966269. S. 242.

76 O petici ze legalizaci DDoS jako formy protestu v USA pojednává *Demanding the right to digitally protest: Hacktivists petition the White House to legalize DDoS.* RT.com [online]. 2013 [cit. 29. 1. 2013]. Dostupné z: http://rt.com/usa/news/us-ddos-attacks-legal-736/?utm_medium=referral&utm_source=t.co.

77 Při jednom z úniků osobních dat ze společnosti Sony např. Sony přiznala, že osobní data uživatelů nebyla žádným způsobem šifrována.
Sony admits personal data was not encrypted. Bit-tech.net [online]. 2011 [cit. 29. 1. 2013]. Dostupné z: http://www.bit-tech.net/news/gaming/2011/04/28/sony-admits-personal-data-was-not-encrypted/1.

78 Zveřejnění osobních údajů zákazníků společností CS Link a Skylink proniklo v prosinci 2012 i do mainstreamových médií.
Hackeři zveřejnili osobní data 57 tisíc zákazníků CS Link a Skylink. Novinky.cz [online]. 2012 [cit. 28. 1. 2013]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/287836-hackeri-zverejnili-osobni-data-57-tisic-zakazniku-cs-link-a-skylink.html.

79 DENNIS, Erin Smith. *A Mosaic Shield: Maynard, The Fourth Amendment, and Privacy Rights in the Digital Age. Cardozo Law Review* [online]. 2011, roč. 33, č. 2, s. 737-771 [cit. 16. 8. 2012]. ISSN 0270-5192. Dostupné z: http://heinonline.org.
HERBERT, Ian. *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence. Berkeley Journal of Criminal Law* [online]. 2011, roč. 16, č. 2, s. 442-505 [cit. 10. 3. 2013]. Dostupné z: http://www.bjcl.org/archives/16_2/herbert_formatted.pdf.

80 Nedostatek českého ekvivalentu zmiňuje i POLČÁK 2012 op. cit., proto autor ponechal výraz v originále. O tomto právu v češtině viz POLČÁK 2012 op. cit., s. 328-329. Obecně pak dále KUHLMANN, Stephanie A. *Do Not Track Me Online: The Logistical Struggles over the right „to be let alone" online. DePaul Journal of Art, Technology & Intellectual Property Law* [online]. 2011, roč. 22, č. 1, s. 229-286 [cit. 16. 8. 2012]. Dostupné z: http://heinonline.org.
V USA sahá historie tohoto práva ve vztahu k informačním technologiím až do roku 1928, kdy Nejvyšší soud USA rozhodoval o legálnosti odposlouchávání telefonních linek federálními agenty bez soudního příkazu. Viz Rozsudek Nejvyššího soudu USA ze dne 4. 6. 1928, ve věci Olmstead v. United States,

V současnosti tedy probíhá intenzivní snaha o zakotvení určitého standardu informačních práv, ať už se jedná o sféru akademickou či o soudní rozhodování nebo o přístup moci výkonné. Jak je výše zmíněno, vzhledem k dynamickému vývoji na poli informačních technologií je téměř nemožné definovat všechny součásti informačního sebeurčení k určitému okamžiku. I přes tento problematický stav je však nepochybné, že pokud má být nějakým způsobem legitimizována kybernetická bezpečnost, musí být veškeré nastavené mechanismy vyvažovány právě za účelem ochrany informačního sebeurčení nebo jejího posílení.

1.3 Povaha kybernetické bezpečnosti

V odborné literatuře můžeme nalézt velké množství nejrůznějších definic a konceptů bezpečnosti, které kopírují vývoj na poli teoretického chápání mezinárodních vztahů.[81] Zároveň se ale dá říci, že pojem bezpečnosti je do určité míry multioborovým fenoménem, který je intenzivně používán v rámci humanitních i technických oborů,[82] a není tedy striktně vázán pouze na politologii, mezinárodní vztahy či bezpečnostní studia.

Bezpečnost může být na jednu stranu definována jako kýžený stav. V rámci Slovníku spisovné češtiny[83] se vyskytuje vazba *„jsoucí bez nebezpečí, bez obav, bez starostí"*, což je negativní vymezení pojmu skrze absenci hrozby. Česká bezpečnostní terminologie běžně pracuje s bezpečností ve formě *„stavu, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (…) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat."*[84] Na druhou stranu může být bezpečnost definována jako vlastnost. S touto (do značné míry technickou) definicí je pracováno v rámci Českého slovníku kybernetické bezpečnosti. Bezpečnost se zde definuje jako *„[v]lastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám."*[85]

Česká legislativa se definice pojmu bezpečnosti dotýká v ustanovení čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.[86] Ustanovení definuje *„zajištění svrchovanosti a územní celistvosti České republiky, ochranu jejich demokratických základů a ochranu životů, zdraví a majetkových hodnot"* za základní povinnosti státu. Vzhledem k teleologii celého zákona se tak dá uvedené přijmout za zákonnou definici bezpečnosti. Tato zákonná definice bezpečnosti pak představuje tzv. národní bezpečnost v rámci české legislativy.[87] Literatura uvádí definici národní bezpečnosti jako *„stav, kdy objektu (národnímu státu jako celku nebo jeho podstatným atributům) nehrozí závažné ohrožení svrchovanosti, územní celistvosti, základům politického uspořádání, vnitřního pořádku a bezpečnosti, životů a zdraví občanů, majetkových hodnot a životního prostředí. Ani jeho spojenci nejsou vystaveni hrozbám, které by v případě jejich aktivace vyžadovaly ozbrojenou či jinou rizikovou spoluúčast. Objekt je schopen a ochoten potenciální hrozby rozpoznat a v maximální možné míře jim zamezovat, popřípadě je eliminovat."*[88] Na první pohled se může zdát, že zákonná definice je do značné míry nekompletní oproti právě uvedené definici národní bezpečnosti. Autor této práce se však domnívá, že vzhledem k mezinárodněprávním závazkům a chování české zahraniční politiky v posledním desetiletí[89] je možné konstatovat, že bezpečnost spojenců je zahrnuta i v rámci zákonné definice v ústavním zákoně č. 110/1998 Sb. Samotnou existenci zákona je také nutné interpretovat tak, že stát je ochoten hrozby potlačovat a zároveň, jelikož veřejná moc musí postupovat v mezích a na základě zákona, je tím zakotvena i jeho schopnost k takovému jednání.

Z ústavního zákona samozřejmě vyplývá přijímání množství dalších dokumentů výkonných orgánů zodpovědných za udržování bezpečnosti České republiky. Definici pojmu bezpečnosti tak obsahuje ve II. Části, 5. odstavci i Bezpečnostní strategie České republiky z roku 2003.[90] Bezpečnostní strategie chápe pojem bezpečnosti jako žádoucí stav (tedy ekvivalenci použitého pojmu *„zajištění"* v zákonné definici), kdy je na *„nejnižší míru sníženo riziko pro ČR plynoucí z hrozeb vůči obyvatelstvu, svrchovanosti a územní celistvosti, demokratickému zřízení a principům právního státu, vnitřnímu pořádku, majetku, životnímu prostředí, plnění mezinárodních bezpečnostních závazků a další definovaným zájmům."* Bezpečnostní strategie České republiky z roku 2011[91] již přímo definici bezpečnosti neobsahuje, ale ve II. Části, 6. odstavci mluví o úkolu vlády ČR a orgánů zajišťovat *„bezpečnost obyvatel, obranu svrchovanosti a územní celistvosti země a zachování náležitostí demokratického právního státu."* Dochází tedy k definici ochraňovaných hodnot, resp. k vymezení okruhu hodnot, proti jejichž ohrožení má vláda i další orgány ČR za úkol zasáhnout.

277 U.S. 438. In: Justia [databáze rozhodnutí]. Justia [cit. 8. 3. 2013]. Dostupné z: http://supreme.justia.com.

Mimo informační technologie je pak možné dostat se až do 19. století. Viz WARREN, Samuel; BRANDEIS, Louis D. *The Right to Privacy. Harvard Law Review* [online]. 1890, roč. 6, č. 5 [cit. 12. 12. 2012]. ISSN 0017-811X. Dostupné z: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

81 Velmi dobře tuto problematiku v českém prostředí shrnuje WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, 2005. 159 s. ISBN 8086898210.

82 ZEMAN, Petr (ed.). Česká bezpečnostní terminologie: výklad základních pojmů [online]. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002 [cit. 16. 10. 2013]. 186 s. ISBN 8021030372. Dostupné z: www.defenceandstrategy.eu/filemanager/files/file.php?file=16048. S. 11.

83 HAVRÁNEK, Bohuslav (red.). *Slovník spisovné češtiny* [online]. Ústav pro jazyk český ČSAV, 2011 [cit. 10. 2. 2013]. Dostupné z: http://ssjc.ujc.cas.cz/.

84 ZEMAN 2002 op. cit., s. 13.

85 JIRÁSEK, Petr; KNÝ, Milan (eds.). *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR & Česká pobočka AFCEA, 2012 [cit. 29. 1. 2013]. ISBN 978-80-7251-378-9. Dostupné z: www.cybersecurity.cz/data/slovnik_v150.pdf. S. 51.

86 Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. Atlas Consulting [cit. 26. 1. 2013].

87 ZEMAN 2002 op. cit., s. 14-15.

88 Tamtéž, s. 15.

89 Viz vysílání vojáků na zahraniční mise.

90 *Bezpečnostní strategie České republiky* [online]. Praha: Pro Ministerstvo zahraničních věcí ČR vydalo ediční oddělení Ústavu mezinárodních vztahů, 2003 [cit. 3. 2. 2013]. 28 s. ISBN 8086345459. Dostupné z: Www.army.cz/assets/files/8492/Bezpe_nostn__strategie__R_-prosinec_2003.pdf.

91 *Bezpečnostní strategie České republiky* [online]. 2011 [cit. 3. 2. 2013]. 21 s. Dostupné z: Www.mzv.cz/file/699914/Bezpecnostni_strategie_CR_2011.pdf.

V případě kybernetické bezpečnosti je situace poněkud složitější. Kybernetická bezpečnost naráží na limity klasického dělení bezpečnosti, tedy dělení na bezpečnost vnitřní a vnější nebo na bezpečnost tvrdou a měkkou. Vnitřní bezpečnost počítá s identifikací a eliminací hrozeb nacházejících se uvnitř objektu, vnější bezpečnost se pak soustřeďuje na identifikaci a eliminaci hrozeb vně objektu. Tvrdá bezpečnost se pak soustřeďuje na hrozby vojenského charakteru a měkká na ostatní.[92] Již ze samotného popisu jednotlivých dělení je patrné (a v rámci dalšího výkladu to bude ještě zdůrazněno), že kybernetická bezpečnost prochází napříč těmito děleními, protože postihuje vojenské i nevojenské použití informačních technologií za účelem útoku na informační systémy. Stejně tak zahrnuje vnitřní i vnější bezpečnostní rizika. Proto je potřeba přijmout ještě další kategorie skrze které bude přesně definována. Bezpečnostní terminologie přímo počítá s přidáním adjektiva (v tomto případě adjektiva „*kybernetický*"), které bude specifikovat charakter ochraňovaného objektu (tedy informačních systémů).[93]

Definici kybernetické bezpečnosti nabízí Český slovník kybernetické bezpečnosti, který definuje kybernetickou bezpečnost jako „*schopnost odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky.*"[94] Tato definice je do jisté míry obecnější než definice pomocí triády CIA[95], protože se zcela vyhýbá specifikaci ideálního stavu, kterého je nutné dosáhnout (tedy právě zajištění důvěrnosti, integrity a dostupnosti systému). Zaměřuje se striktně na faktický stav nenarušitelnosti zvnějšku či na schopnost rychlé nápravy případných škod.[96] Dále je nezbytné si uvědomit dichotomii pojmů „*safety/security*" v anglickém jazyce[97], která do určité míry zohledňuje intencionalitu či neintencionalitu provedeného útoku. Zatímco výraz „*safety*"[98] směřuje k zohlednění jedince a jeho možného ohrožení nedbalostí, „*security*"[99] se týká především hrozeb intencionálních.[100] Dle definice v Českém slovníku kybernetické bezpečnosti tedy originální pojem „*Cyber Security*" zahrnuje jak „*safety*", tak i „*security*."

Kybernetická bezpečnost musí být chápána jako složená z prvků tzv. triády CIA[101] – tedy jako zajištění důvěrnosti (*confidentiality*), integrity a dostupnosti (*availability*) informačního systému.[102] Triádu CIA bylo možno v minulosti nalézt v rámci českého právního řádu v ustanovení §8, odst. 1 Vyhlášky Národního bezpečnostního úřadu č. 56/1999 Sb.[103] Tento předpis byl zrušen zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, kde se ale také zmínka o triádě CIA vyskytuje, konkrétně v ustanovení §5, písm e).[104] S triádou CIA již při definici kybernetické bezpečnosti se můžeme setkat i v některých dokumentech Evropské komise.[105]

Důvěrnost se v rámci triády CIA vztahuje k ochraně uložených či přenášených dat před přístupem ze strany neautorizovaných osob.[106] Pro zajištění důvěrnosti musí být možné zamezit některým uživatelům v přístupu k informacím, dále musí mít systém možnost ověřit totožnost uživatele, který k informacím hodlá přistupovat a vyhodnotit, zda-li má dostatečné oprávnění či nikoli. Autentizace a autorizace tak představují inherentní součást důvěrnosti systému, protože bez nich není možné ověřit totožnost entity (autentizace) a vyhodnocení oprávněnosti takového přístupu (autorizace). Nejjednodušším způsobem je tak ukládání informace na bezpečném počítači, ke kterému mají fyzický přístup pouze osoby náležitě prověřené a pověřené. Pokud pak informace opouští takovýto počítač, je nutné ji šifrovat.[107]

Kromě ochrany informačního systému přímo proti hrozbám přicházejícím skrze informační sítě je nutné myslet na zajištění důvěrnosti proti hrozbám v rámci aktuálního světa – součástí důvěrnosti informačního systému je tedy i systém nakládání s hesly, opatrnost při

92 ZEMAN 2002 op. cit., s. 12.

93 Tamtéž, s. 12.

94 JIRÁSEK 2012 op. cit., s. 68.

95 Vysvětlení pojmu dále v textu.

96 Tedy i jinak nezabezpečená síť (tedy nedisponující důvěrností, integritou a dostupností) může být dle této definice považována za bezpečnou, pokud je nenarušitelná zvnějšku a je schopná rychle napravit případné škody a dosáhnout uvedení do původního stavu.

97 Potažmo sécurité/sûreté v jazyce francouzském.

98 Sûreté.

99 Sécurité.

100 ZEMAN 2002 op. cit., s. 11.

101 Alternativu k triádě CIA představuje tzv. Parkerova šestice (angl. Parkerian hexad), která pracuje s šesti elementy informace. Jedná se o důvěrnost (confidentiality), držení či kontrolu (possession or control), integritu, autentičnost (authenticity), dostupnost (availability) a užitečnost (utility). Autorem tohoto dělení je Donn B. Parker, který kritizuje triádu CIA jako nedostatečnou pro popis zajištění bezpečnosti informací vně i uvnitř informačních sítí. Parkerova šestice v současnosti představuje spíše menšinový koncept.
BOSWORTH, Seymour; KABAY, M. E. (eds.). *Computer Security Handbook.* 4th Edition. Hoboken: John Wiley & Sons, 2002. ISBN 0471412589. S. 116-136.

102 GRAHAM, James; HOWARD, Richard; OLSON, Ryan (eds.). *Cyber Security Essentials*. Boca Raton: CRC Press, 2011. 325 s. ISBN 978-1-4398-5123-4. S.1.

103 *„Pro každý informační systém musí být již v počáteční fázi jeho vývoje zpracována bezpečnostní politika informačního systému. Bezpečnostní politiku informačního systému tvoří soubor norem, pravidel a postupů, který vymezuje způsob, jakým má být zajištěna* ***důvěrnost, integrita a dostupnost*** *utajované informace a odpovědnost uživatele za jeho činnost v informačním systému. Zásady bezpečnostní politiky jsou rozpracovány v projektové a provozní bezpečnostní dokumentaci informačního systému."* [zvýraznění autor]
Vyhláška Národního bezpečnostního úřadu č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu. In: *CODEXIS* [právní informační systém]. Atlas Consulting [cit. 10. 2. 2013].

104 *„[B]ezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit* ***důvěrnost, integritu a dostupnost*** *utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému (...)[.]"* [zvýraznění autor]
Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: CODEXIS [právní informační systém]. Atlas Consulting [cit. 10. 2. 2013].

105 *„Network and information security can thus be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the* ***availability, authenticity, integrity and confidentiality*** *of stored or transmitted data and the related services offered by or accessible via these networks and systems."* [zvýraznění autor]
Comm(2001)298, Network and Information Security: Proposal for European Policy Approach. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 12. 3. 2013]. Dostupné z: http://eur-lex.europa.eu/. S. 5

106 GRAHAM 2011 op. cit., s. 4.

107 V úvahu tak připadá přenos po VPN (automaticky šifruje přenos mezi dvěma koncovými body) nebo šifrování e-mailů, šifrování dat umístěných na přenositelných discích atd.

zadávání hesel při přístupu k systému, nakládání se šifrovacími klíči atd., tedy celá struktura bezpečnostních procesů, vzdělání a obecné prevenční povinnosti uživatelů majících přístup k systému. Důvěrnost je základním stavebním kamenem soukromí v informačních sítích a ochrany osobních údajů tamtéž. Bez zajištění důvěrnosti není možné o ochraně soukromí či osobních údajů ani hovořit, proto je vytvoření a posílení mechanismů směřujících k zajištění větší důvěrnosti informačních sítí tak esenciální. Musí být jednou z primárních snah při zajištění jakékoli národní strategie kybernetické bezpečnosti.[108]

Integrita pak představuje vlastnost systému, kdy je znemožněno nepozorovaně změnit data.[109] Velice úzce souvisí s již zmíněnou autorizací a autentizací (systém tedy musí mít možnost autorizace a autentizace uživatelů), ale i s tzv. nepopiratelností.[110] Integrita systému je podstatná i pro právní jistotu uživatelů – souvisí s identifikací celého řetězu od původce zprávy přes obsah zprávy až k identitě příjemce. Zajišťuje kompletnost uložených a přenášených dat. V případě, že dojde ke změně těchto dat, v systému to musí být možné zpozorovat. Poslední složkou triády CIA je dostupnost. Je možné ji stručně shrnout jako požadavek, aby data v systému (či celý systém) byl dostupný ve chvíli, kdy je to potřebné. Je nutné zajistit spolehlivý přístup k datům a informačním službám a adekvátní odezvu systému na požadavky oprávněných uživatelů.[111]

Terminologické problémy způsobuje používání pojmu informační bezpečnosti, který je částí veřejnosti chápán jako pojem libovolně zaměnitelný s pojmem kybernetické bezpečnosti, i když se o pojmy ekvivalentní zcela jistě nejedná. Informační bezpečnost je také definována triádou CIA, ale nejedná se striktně o bezpečnost v rámci informačních sítí, nýbrž i mimo ně (tedy i o zabezpečení tištěných dokumentů, nakládání s nimi atp.). Pojem informační bezpečnosti je tedy pojmem širším než bezpečnost kybernetická. Tímto bohužel terminologické problémy nekončí. Termín kybernetické bezpečnosti je používaný v rámci přípravy nové české legislativy i v některých dalších zemích. NATO ale pracuje s termínem kybernetické obrany, EU potom s termíny jako je bezpečnost sítí a informací, informační bezpečnost *(sic!)*, ICT bezpečnost atd. Jedním z prvních kroků kýžené mezinárodní regulace[112] by tak mělo být sjednocení používané terminologie.[113]

Při popisu a právní konstrukci jakékoli bezpečnosti je, bez ohledu na akceptovanou definici bezpečnosti, absolutně nezbytné uvědomit si povahu bezpečnosti jako nedistributivního práva. V případě kybernetické bezpečnosti se pak z právně-teoretického hlediska jedná o nedistributivní informační právo.[114] Jak již bylo zmíněno dříve v tomto textu, kybernetická bezpečnost by bez ochrany relevantních distributivních práv nemohla být legitimní. *Per se* tedy kybernetická bezpečnost nemůže a nesmí existovat. Nedistributivní informační práva představují veřejná informační dobra, která pak představují v kontinentální Evropě[115] množinu pravidel nedělitelných na jednotlivé subjekty. K tomuto se v minulosti vyjadřoval i Ústavní soud ve svém Nálezu sp. zn. Pl. ÚS 32/95[116] ze dne 3. 4. 1996, kdy poznamenal, že *„[v]eřejným statkem se tudíž určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly.“* Veřejné dobro je tedy v důsledku směřováno k jednotlivci, ale není ve své podstatě individuálně ochraňováno – jeho ochrana má státní charakter.[117] Nedistributivní práva jsou odlišným způsobem pojata v rámci angloamerického právního systému. Zde fungují na premise oddělení státu a práva – jedná se o práva distributivní, ale jejich oprávněným subjektem je stát. Tato práva státu náleží jako subjektu a stát je zároveň nadán i aktivní legitimací k jejich vymáhání.[118]

Za nejpalčivější aspekty rychlého technologického vývoje a informatizace společnosti jsou v současnosti považovány problémy související s distributivními právy. Aspekt nedistributivních práv, resp. změnění možnosti státu dostát své primární odpovědnosti zajišťovat společenskou reprodukci ochranou distributivních práv prosazováním práv nedistributivních, je často opomíjen. Zajišťování společenské reprodukce je přitom jednou ze základních materiálních funkcí státu.[119] Nízká politická vůle k prosazování vhodné právní regulace je způsobena nízkým společenským zájmem, ale také určitým

108 Komise v minulosti deklarovala, že bude nadále podporovat aktivity na tomto poli, zejména zaváděním protokolů IPSec a IPv6 do praxe. Zavedení IPv6 tedy Komise chápe nejenom jako zajištění rozvoje informační společnosti, ale i zajištění větší míry důvěrnosti internetu, protože používání IPv6 přímo ovlivňuje použitelnost IPSec v praxi.
Comm(2001)298 2001 op.cit., s. 19.

109 GRAHAM 2011 op. cit., s. 4-5.

110 Angl. Nonrepudiation. Jedná se o ověření úkonu, který byl proveden prostřednictvím informačních sítí. Zahrnuje potvrzení původce a zároveň i nezměnění informací při přenosu. Je zajišťována především asymetrickým šifrováním (soukromý klíč k podpisu, veřejný klíč k ověření pravosti podpisu) či hašováním zprávy. Nástrojem pro zajištění je samozřejmě také elektronický podpis známý i v České republice (zákon č. 277/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů).
GRAHAM 2011 op. cit., s. 3.

111 Tamtéž, s. 5-6.

112 Mezinárodní telekomunikační unie např. zmiňuje, že bez mezinárodní regulace jsou národní strategie směřující k posílení kybernetické bezpečnosti jako vlastnosti a udržení kybernetické bezpečnosti jako stavu nutně méně efektivní.
ITU National Cybersecurity Strategy Guide [online]. 2011 [cit. 1. 10. 2012]. 119 s. Dostupné z: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf. S. 37.

113 TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. *International Cyber Incidents: Legal Considerations* [online]. Tallinn: CCD COE Publications, 2010 [cit. 15. 5. 2012]. 130 s. ISBN 978-9949-9040-0-6. Dostupné z: http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. S. 101-102.

114 Polčák mluví o *„nedistributivním právu s dominantně informačním charakterem.“* POLČÁK 2012 op. cit., s. 343.

115 Tedy za podmínky ztotožnění státu s jeho právním řádem.

116 Nález Ústavního soudu ČR ze dne 3. 4. 1996, sp. zn. Pl. ÚS 32/95. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

117 Právě zde tedy existuje dělící linie mezi základními právy a svobodami a veřejnými dobry, jak je ostatně uvedeno i v již zmíněném Nálezu Ústavního soudu sp. zn. Pl. ÚS 32/95 ze dne 3.4.1996.

118 BENTHAM, Jeremy. *Leviathan* [online]. Project Gutenberg, 2002 [cit. 1. 2. 2013]. Dostupné z: http://www.gutenberg.org/.

119 HOLLÄNDER, Pavel. *Základy všeobecné státovědy.* 3. vydání. Plzeň: Aleš Čeněk, 2012. 429 s. ISBN 9788073803957. S. 103-106.

odporem společnosti k omezování distributivních práv v zájmu práv nedistributivních. Tato výhrada se týká hlavně postkomunistických zemí, kde docházelo v zájmu nedistributivních práv k masivnímu omezování práv distributivních.[120] Nicméně po událostech z 11. 9. 2001 se i v USA a v demokraciích Západní Evropy diskutuje zajištění bezpečnosti a boj proti terorismu jako určitá opozice k osobním svobodám, hlavně pak v otázce reálné implementace bezpečnostní politiky orgány státu.[121] Dá se uzavřít, že v současné době je důležité nejen intenzivně se zabývat proporcionalitou aplikace distributivních a nedistributivních informačních práv. Stejná důležitost by měla být v českých podmínkách (a obecně v podmínkách postkomunistických zemí) kladena zároveň i na osvětovou a propagační činnost. Zejména prostředí internetu je veřejností vnímáno jako nespoutaný prostor, kde stát nemůže a nesmí zasahovat. Nicméně při zajišťování bezpečnosti (tedy nedistributivního informačního práva) je nutné solidárně omezit individuální svobody jednotlivce (tedy distributivního informačního práva, které je integrální součástí katalogu informačního sebeurčení). Tento názor pak musí být veřejnosti náležitým způsobem komunikován tak, aby si uvědomila závažnost hrozeb.

Bohužel momentálně neexistuje celospolečenský[122] konsenzus nad mírou přípustnosti tohoto solidárního omezení individuální svobody v prostředí informačních sítí za účelem zajištění bezpečnosti. Při posuzování konfliktu jednotlivých distributivních práv či při posuzování konfliktu distributivního a nedistributivního práva je nutné přihlédnout k proporcionalitě zvoleného řešení. Dílčí komponenty zásady proporcionality vyložil český Ústavní soud v Nálezu sp. zn. Pl. ÚS 4/94 ze dne 12. 10. 1994.[123] Jedná se o kritérium vhodnosti, kritérium potřebnosti a porovnání závažnosti obou v kolizi stojících práv. V této souvislosti se také zmiňuje tzv. příkaz k optimalizaci[124] jako využití všech možných prostředků minimalizace omezení jednoho z práv v případě priority jednoho z nich. Zejména při rizicích plynoucích z asymetrických konfliktů[125] se může příkaz k optimalizaci snadno změnit v test vyloučení extrémní disproporcionality.

Druhá jmenovaná možnost zásadním způsobem omezuje smysl testu proporcionality, který nadále vylučuje pouze prostředky k prosazení nedistributivního práva vedoucí k absolutní likvidaci práva distributivního.[126] Jako příklad je možné uvést situaci v USA po útocích z 11. 9. 2001, kdy se zcela změnila strategie veřejné moci ve vztahu k ochraně národní bezpečnosti. Došlo k exponenciálnímu nárůstu sbíraných a uchovávaných dat jak do rozsahu, tak do charakteru. NSA[127] tehdy zahájila preventivní odposlechy telefonních hovorů, dále byla shromažďována data ze zdravotnictví, bankovnictví, vzdělávání, ale i z databází soukromých obchodních společností za účelem jejich analýzy a využití při boji proti terorismu. Ač bylo původně deklarováno postupné omezování těchto aktivit, aféra kolem programu PRISM dává tušit, že realita je jiná. Tyto aktivity představují odstrašující snahu státu zvýhodnit své postavení při zajištění národní bezpečnosti v rámci asymetrického konfliktu.[128]

Lze konstatovat, že proporcionalita musí být integrální součástí jakéhokoli uvažování na bezpečnostní témata, aby nedošlo k příliš širokému nastavení pravomocí ve prospěch exekutivy a neprospěch uživatelů, resp. jejich distributivních práv. Na druhou stranu se ale absence úpravy kybernetické bezpečnosti, která by sledovala pevné principy, také negativně podepisuje na distributivních právech jednotlivců. Soukromé společnosti, které vlastní majoritu kritických informačních infrastruktur, se dostávají do bezprecedentní pozice moci a vlivu na osobní životy uživatelů služeb. Nulová varianta v podobě, v jaké s ní původně pracoval Věcný záměr zákona o kybernetické bezpečnosti,[129] tak byla z tohoto důvodu seznána stejně nevhodnou, jako excesivní pravomoci svěřené exekutivní moci.

V českých podmínkách nebyla bezpečnostní situace nikdy tak dramatická, aby ospravedlňovala podobné neproporcionální zásahy či dokonce dočasné potlačení distributivních práv za účelem zajištění práv nedistributivních. Přesto velký zájem veřejnosti vzbudil případ „transpozice"[130] Směrnice Evropského parlamentu a Rady 2006/24/ES v podobě zákona č. 127/2005 Sb., o elektronických komunikacích. K porušení proporcionality zde došlo tak flagrantním a zcela zásadním způsobem, že se nabízí otázka povahy nebezpečí, před kterým mělo plošné a preventivní uchovávání provozních údajů poskytovat ochranu. Ústavní soud nakonec §97, odst. 3 a §97, odst. 4 napadeného zákona zrušil a zrušil i související prováděcí předpis, kterým byla vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.[131] Jedním z opěrných bodů argumentace Ústavního soudu bylo, že již prosté takto široce nastavené uchovávání provozních a lokalizačních údajů je způsobilé zasahovat protiústavně do soukromí jednotlivců. Státní

120 Pro podrobnější deskripci českého postoje např. BOBEK, Michal; MOLEK, Pavel; ŠIMÍČEK, Vojtěch (eds.). *Komunistické právo v Československu: Kapitoly z dějin bezpráví.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009. 1005 s. ISBN 9788021048447. S. 330-363.

121 ISANGA, Joseph M. *Counter-Terrorism and Human Rights: The Emergence of a Rule of Customary International Law from United Nations Resolutions. Denver Journal of International Law and Policy* [online]. 2009, roč. 37, č. 2, s. 223-255 [cit. 29. 6. 2012]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2093414.

122 A v podstatě ani částečný.

123 Nález Ústavního soudu ČR ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

124 ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. 212 s. ISBN 9788021054493. S. 23.

125 Tedy nahrazení střetů stát vs. stát terorismem, kybernetickými útoky skupin různého charakteru atd.

126 ŠIMÍČEK 2011 op. cit., s. 28-30.

127 National Security Agency.

128 ŠIMÍČEK 2011 op. cit., s. 136-138.

129 *Věcný záměr zákona o kybernetické bezpečnosti* [online]. 2013 [cit. 15. 10. 2013]. Dostupné z: http://www.nbu.cz/download/nodeid-1216/.

130 Směrnice byla totiž vydána později než český zákon.

131 Nález Ústavního soudu ČR ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10. In: *NALUS* [databáze rozhodnutí Ústavního soudu]. Ústavní soud [cit. 8. 3. 2013]. Dostupné z: http://nalus.usoud.cz/Search/Search.aspx.

orgány totiž mají potenciální možnost si údaje vyžádat a restriktivně stanovená pravidla přístupu nejsou schopna zhojit vadu v podobě uchovávání provozních údajů tak značného rozsahu.

Poslední otázkou související s povahou kybernetické bezpečnosti je současný celosvětový trend privatizace základních funkcí státu, zejména pak bezpečnosti. Konec Studené války a snižování armádních stavů uvolnil na celém světě množství vojenských expertů hledajících obživu. Soukromé vojenské společnosti pracují v Iráku a v Afghánistánu pro vládu USA, jejich služeb využíval libyjský vůdce Muammar Kaddáfí[132] a na světě jich tak dnes existuje značné množství. Potřeba existence těchto skupin je často zdůvodňována omezeností rozpočtů na zajišťování bezpečnosti a také lepším *public relations* při nasazování soukromých kontraktorů do rizikových operací, jelikož smrt vojáků znevýhodňuje armádu v boji s veřejným míněním. K privatizaci bezpečnosti dochází hlavně v oblastech angloamerické právní kultury, protože filosofické zdůvodnění přenosu výkonu bezpečnosti na soukromé subjekty je jednodušší než v rámci práva kontinentálního. Vzhledem k povaze bezpečnosti jako distributivního práva se státem jako oprávněným subjektem se při přenosu povaha bezpečnosti nijak nemění, pouze se mění oprávněný subjekt.

V kontinentálním právu je nutná konstrukce hybridní formy nedistributivního práva se znaky práva distributivního, které je pak možné přiřadit jednotlivým subjektům.[133] Vzhledem k povaze internetu a limitovaným možnostem vynutitelnosti práva se použití soukromých subjektů při zajištění bezpečnosti jeví jako vhodné a jediné možné řešení. Kritické informační infrastruktury, které představují soustavu systémů, infrastruktur, sítí a služeb ICT, jejichž narušení, zničení nebo nedostupnost by měla vážný dosah na fungování dalších sektorů a životně důležitých společenských funkcí, včetně národní bezpečnosti, jsou totiž převážně v soukromých rukou. Např. v USA podíl těchto infrastruktur kolísá od 80% do 95%.[134] Podobně ke stavu přistupoval i Věcný záměr zákona o kybernetické bezpečnosti, kdy konstatoval, že informační systémy a komunikační infrastruktura veřejné správy představuje pouze podmnožinu informačního systému a služeb informační společnosti, který je nezbytný k efektivnímu fungování společnosti.[135] V případě nezapojení soukromoprávních subjektů do aktivní kybernetické bezpečnosti tedy hrozí, že stát nedostojí své povinnosti zajistit bezpečný provoz vitálních funkcí státu, případně nedostojí ani svým mezinárodním závazkům.[136]

Problémem je i v tomto případě proporcionalita, tedy zhodnocení míry v jaké je možné přenášet na soukromoprávní subjekty odpovědnost za zajištění bezpečnosti ve vztahu k jejich vlastnickým právům. Podnikatelský sektor funguje zaměřen na cos*t-effective* přístup a vynucovat si maximální možné zabezpečení se proto nejeví jako vhodné. Soukromě vlastněné kritické infrastruktury tak mohou představovat, vzhledem k nižšímu zabezpečení oproti infrastruktuře veřejného sektoru, snadnější přístup pro potenciálního útočníka při narušení národní infrastruktury.[137] Komunikace veřejného sektoru se sektorem soukromým při návrhu strategie či přímo při tvorbě zákona o kybernetické bezpečnosti se tedy jeví jako žádoucí. Účelem je nejenom zajištění jakékoli bezpečnosti, ale zajištění kybernetické bezpečnosti v míře, která by nebyla neustále napadána soudní cestou pro neproporcionální zatížení soukromého sektoru.

2. Hrozby a nástroje ochrany

2.1 Změny bezpečnostních hrozeb

Existenci hrozeb proti distributivním právům v rámci informační společnosti lze poměrně snadno empiricky prokázat na nárůstu frekvence a závažnosti jednotlivých bezpečnostních incidentů na úseku ochrany informačních systémů. Na změny společnosti totiž reagují kromě běžného společenského vývoje vývojem i jevy vnímané negativně, tedy mimo jiné nedbalostní jednání, kriminalita, terorismus i strategie použité ve vojenských konfliktech. Jak se zvyšuje závislost společnosti na informačních systémech bez jejich adekvátního zabezpečení, zvětšuje se i možnost jejich napadení za různými účely.

Bezpečnostní incidenty jsou často označované jako kybernetické útoky, což v právním prostředí vzbuzuje určitou terminologickou nepříjemnost. Útok jako takový je totiž předmětem mezinárodního práva a předpokládá vojenský konflikt, což zdánlivě diskvalifikuje jeho použití jako zobecňujícího pojmu.[138] Podle některých autorů je tento problém ale pouze virtuální a pojem kybernetický útok se ujal jako generální pojem veškerých kybernetických hrozeb namířených proti informačním systémům. V tomto duchu pak bude termín kybernetický útok používán i v této práci – jako obecný pojem zastřešující všechny typy kybernetických hrozeb, tedy nejenom použití kybernetických operací v rámci válečných konfliktů.

Kybernetické útoky mohou být děleny mnoha různými způsoby. Prvním z vybraných pro tuto práci, který se velmi často vyskytuje při vytváření statistik, je dělení na kyberkriminalitu, hacktivismus, kybernetickou válku a kybernetickou špionáž.[139] Rozdělení reflektuje motivaci původců těchto útoků, kdy kyberkriminalita směřuje k vlastnímu obohacení, hacktivismus na upozornění na určitý problém formou apelu, kyber-

132 MICHAELS, Jon D. *Private Military Firms, American Precedent, and the Arab Spring. Stanford Journal of International Law* [online]. 2012, roč. 48, č. 2, s. 277-288 [cit. 19. 10. 2013]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2160550. S. 277.

133 POLČÁK 2012 op. cit., s. 342.

134 BASTL 2007 op. cit., s. 107.

135 Věcný záměr 2012 op. cit., s. 18.

136 Tamtéž, s. 61.

137 BASTL 2007 op. cit., s. 107-108.

138 SOLCE, Natasha. *The Battlefield of Cyberspace: The Inevitable New Military branch – The Cyber Force. Albany Law Journal of Law & Technology* [online]. 2008, roč. 18, č. 1, s. 293-324 [cit. 16. 8. 2012]. ISSN 1059-4280. Dostupné z: http://heinonline.org. S. 300-302.

139 S tímto dělením pracuje např. Hackmageddon.com. Viz *2012 Cyber Attacks Statistics* [online]. 2013 [cit. 7. 2. 2013]. Dostupné z: http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/.

netická válka k poškození infrastruktury jiným státem či nestátním aktérem a kybernetická špionáž k získání jinak nedostupných informací v obchodním či mezinárodním styku.

Druhým je pak popis pomocí spektra bez jasných hranic mezi jednotlivými skupinami, které zahrnuje porušení vnitřních nařízení; porušení právní povinnosti; kybernetickou kriminalitu; kybernetický terorismus; kybernetickou válku.[140] Toto spektrum představuje velice příhodnou konstrukci umožňující popisovat jednotlivé útoky skrze nejednoznačné pojmy (jakousi polohu ve spektru) a postupně při zvyšování vážnosti zapojovat jednotlivé složky systému na zajištění kybernetické ochrany. Zatímco v reálném světě je totiž velice krátce po události jasné, zdali se jednalo o kriminální či teroristickou činnost nebo dokonce narušení suverenity jiným státem, v kyberprostoru tak snadná identifikace neexistuje. Stírají se hranice mezi vojenskými orgány a orgány vynucujícími právo. Porušení vnitřního nařízení tak může představovat např. neopatrné nakládání s hesly či neaktualizování firemního bezpečnostního softwaru. Porušení právní povinnosti se týká např. nenahlášení bezpečnostního incidentu ze strany ISP.[141] Kyberkriminalita je pak představována jednáním vedoucím k osobnímu prospěchu, bez ohledu na to, zdali se jedná o formu zvláštní skutkové podstaty[142] nebo o obecný pojem představující kriminální činnost za použití moderních technologií.[143] Kybernetický terorismus pak představuje ohrožení samotného chodu kritických informačních systémů ze strany nestátního aktéra,[144] kybernetická válka pak ohrožení ze strany aktéra státního. Nejde tedy o motivaci přestupce, ale spíše o povahu či intenzitu a ve spektru jsou zahrnuty i možné incidenty neúmyslného charakteru. Důležitým aspektem hodnocení hrozeb kromě jejich povahy jsou použité nástroje. Bez ohledu na to, ve které části spektra se případný útok nachází, použité nástroje zůstávají téměř bezvýhradně stejné, liší se jenom v míře své sofistikovanosti.[145] Počítačové viry, logické bomby, DDoS útoky, phishing hesel a další taktiky[146] mohou být použity jak vojenským tak nevojenským sektorem, mohou být použity v rámci kybernetické kriminality, ale i konkurenčního boje. Zatímco si lze jen těžko představit, že na obchodního konkurenta někdo vytáhne za bílého dne zbraň, špionážní taktiky se ale stávají každodenní realitou, před kterou je nezbytné systém chránit. Právě jednotnost zbraní se tak stává dalším způsobem klasifikace jednotlivých hrozeb – skrze nástroje, kterých používají.[147]

V oblasti kybernetické kriminality již v současnosti registrujeme určité snahy směřující k její prevenci a jejímu potlačení. EU plánuje otevřít Evropské centrum pro boj proti kybernetické kriminalitě, na stránkách Policie ČR je možné v online formuláři nahlásit bezpečnostní incident,[148] existuje Úmluva Rady Evropy o kyberkriminalitě atd. Český trestní zákoník pak přímo obsahuje ustanovení o neoprávněném přístupu k počítačovému systému a nosiči informací.[149] Bohužel se ve spektru hrozeb jedná o jedinou alespoň částečně legislativně přímo upravenou oblast, a to ještě poměrně překotně, kdy se harmonizačním snahám na mezinárodní úrovni věnuje vícero organizací.[150] Na nejnižší úrovni spektra je zřejmě možné vystačit si se vztahy pracovněprávními, při outsourcingu správcovských činností pak obchodněprávními. Při porušení právních povinností se již přímo počítá se zakomponováním povinnosti hlásit bezpečnostní incidenty ústřednímu dohledovému pracovišti.[151] Nejzajímavější výzvy z hlediska výzkumu a typologie hrozeb se nacházejí v nejvyšších částech spektra, tedy na úrovni kyberterorismu a kybernetické války. Kyberterorismus může vést k zásadnímu ohrožení národní bezpečnosti v rámci ze strany nestátních či polostátních aktérů a zároveň představuje z hlediska bezpečnostních studií terminologický problém.[152]

Kybernetická válka je součástí vojenských doktrín, což předpokládá její určitou institucionalizaci za účelem efektivního využití ve vojenském konfliktu. Poprvé se technologická změna v oblasti vojenských operací materializovala na českém území v rámci Revoluce ve vojenských záležitostech[153], která byla definována jako *„významná změna v charakteru vedení války vyvolaná inovativním uplatněním nových technologií, která ve spojení s dramatickými změnami ve vojenské doktríně a operační a organizační koncepci zásadně mění způsob a provádění vojenských operací.“*[154] Jedním z cílů RMA je tak dosažení a udržení informační nadvlády v rámci konfliktu, což úzce souvisí jak s napadáním informačních systémů nepřítele, tak i s ochranou informačních systémů vlastních.

Doktrínou, která se soustředí na boj v informačních sítích je pak Network Centric Warfare.[155] Tato doktrína

140 TIKK, Eneken. *Comprehensive Legal Approach to Cyber Security* [online]. Tallinn, 2011 [cit. 3. 9. 2012]. 170 s. Disertační práce, University of Tartu, Právnická fakulta. ISBN 978-9949-19-763-7. Dostupné z: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1. S. 69.

141 S hlášením pracoval i Věcný záměr 2012 op. cit., s. 43 a povinnost byla implementována v rámci ustanovení §9 *Návrhu zákona o kybernetické bezpečnosti* [online]. 2013. [cit. 16. 10. 2013]. Dostupné z: http://www.nbu.cz/download/nodeid-1055/.

142 Jedná se o ustanovení §§230 až 232 Trestního zákoníku.

143 BAGGILI, Ibrahim (ed.). *Digital Forensics and Cyber Crime*. New York: Springer, 2011 [cit. 15. 9. 2011]. 157 s. ISBN 978-3-642-19513-6. S. 2-4.

144 Nemusí se nutně jednat pouze o formu terorismu. Ke zmíněnému efektu může vést kriminální činnost masivního rozsahu atp.

145 Rozdíl mezi sofistikovaným malwarem jako je Stuxnet nebo Red October a „běžným“ červem z kancelářského počítače je zcela očividný.

146 Popis různých technik proniknutí do systémů či zneužití uživatelovi nepozornosti obsahuje publikace GRAHAM 2011 op. cit., s. 75-266.

147 ŚWIĄTKOWSKA, Joanna (ed.). *V4 cooperation in ensuring cyber security – analysis and recommendations.* Kraków: The Kosciuszko Institute, 2012. 85 s. ISBN 9788393109364. S. 21-30.

148 Viz http://aplikace.policie.cz/hotline/.

149 §230 Trestního zákoníku.

150 TIKK, Eneken. *Ten Rules for Cyber Security. Survival: Global Politics and Strategy* [online]. 2011, roč. 53, č. 3, s. 119-132 [cit. 1. 8. 2012]. ISSN 1468-2699. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2011.571016. S. 129.

151 Pozn. pod čarou 141.

152 K pojmu a jeho možným vymezením BASTL 2007 op. cit., s. 118-122.

153 Angl. Revolution in Military Affairs.

154 KOZÁK, Karel. *Revoluce ve vojenských záležitostech. Vojenské rozhledy.* 2001, roč. 10, č. 4, s. 67-84. ISSN 1210-3292.

155 K vymezení pojmu a jeho povaze ALBERTS, David; GARTSKA, John; STEIN, Frederick. *Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd Edition (revised).* Washington: CCRP Press, 1999. 287 s. ISBN 1-57906-019-6. S. 88-93.

vychází z předpokladu, že válčení v prostředí informační společnosti má jiný charakter než v minulosti a proto vyžaduje nové přístupy. Tomuto trendu efektivněji přizpůsobují obchodní společnosti, mající např. síťovou hierarchickou strukturu, které pak mají výhodu v konkurenčním boji. Se stejnou optikou je pak nutno přistupovat i k armádám v rámci NCW. Maximalizace zesíťování systémy včasné výstrahy v dispozici jednotlivců a dalšími nástroji zvyšují synchronizaci a efektivitu bojové činnosti. Zajišťují informační dominanci, zároveň ale představují přirozené cíle pro nepřítele a vyžadují tedy zajištění bezpečnosti.

Na asymetrický konflikt pak reaguje doktrína Fourth Generation Warfare,[156] která počítá s protivníkem neochotným jít do přímého střetu. Takovýto protivník bude napadat informační systémy diverzní činností na úrovni teroristických akcí a používat je jako sociální či politický apel v rámci nátlakové činnosti cílené na oslabení bojové morálky. Jakkoli se mohou tyto vojenské teorie a doktríny zdát nepoužitelné pro chápání kybernetické bezpečnosti civilního sektoru, jsou pro pochopení její role velice podstatné. Obrovská část našich životů se přesouvá do prostředí informačních sítí a tyto informační sítě se stávají i cílem různorodých vojenských operací. Na rozdíl od konfliktů minulých, kdy bylo jednoznačně možné odlišit školu od továrny na munici, kritické informační struktury nejsou takovým způsobem odlišitelné. Představují informační dálnici pro civilní i vojenskou složku státu a narušením či přerušením jejich činnosti nikdy nedojde k zastavení pouze civilního či pouze vojenského sektoru.[157] Vojenské systémy musí samozřejmě být náležitě zabezpečeny, tedy na nejvyšší možné úrovni, proti použití určitých sofistikovaných metod průniku nebo poškození systému.[158] Ale i neveřejný sektor musí rizika reflektovat, vzhledem k chybějícímu mezinárodnímu konsensu nad samotnou povahou vedení kybernetické války.[159]

V souvislosti s nárůstem počtu kybernetických útoků,[160] jejich sofistikovanosti, ale i mediální pozornosti, které se jim dostává, se často vyskytuje označování bezpečnostních incidentů jako prvních svého druhu. Estonské události z dubna 2007 jsou označovány jako první případ kybernetické války vedené suverénním státem proti státu jinému a malware Stuxnet pak byl označen za první útok svého druhu na kritické infrastruktury, které jsou základem moderních ekonomik.[161]

Za opravdu prvním incidentem, kdy bylo použito metod kybernetického útoku k narušení kritické infrastruktury, zřejmě stála CIA. V 80. letech 20. století probíhala ze strany SSSR špionáž značného rozsahu v Kanadě a USA za účelem získání moderních západních technologií. CIA při své akci podstrčila KGB nejenom vadné plány na výrobu součástek, ale i software obsahující logickou bombu, což nakonec vedlo k rozsáhlé explozi plynovodu v odlehlých oblastech Sibiře.[162] Motorem opravdového zájmu o kybernetickou bezpečnost však byl právě duben 2007 v Estonsku, který zcela odhalil zranitelnost masivně informatizované společnosti při kybernetickém útoku. V řádu hodin se útočníkům podařilo vyřadit informační systémy bankám, novinám i vládním institucím.[163] Někteří estonští představitelé dokonce zvažovali aktivaci Článku 5 Severoatlantické smlouvy,[164] což by se stalo poprvé v historii za účelem ochrany informačních sítí a nikoli fyzického útoku.[165] K aktivaci nakonec nedošlo, přesto se akce přímo v Tallinnu účastnili experti NATO. Jejich činnost však nebyla tak efektivní, jak být měla. K tomu došlo převážně z důvodu, že většina kritických informačních infrastruktur, které byly napadeny, byla v soukromých rukou a exekutiva státu tak nad nimi neměla žádnou moc. Právě tehdy si NATO uvědomilo zásadní nedostatky v zajištění kybernetické bezpečnosti své i svých členů, což vedlo mj. i k vytvoření Centra excelence zaměřeného na kooperativní kybernetickou bezpečnost na úrovni NATO.[166]

Další incident podobného rozsahu se udál v roce 2008, kdy byly v rámci války v Gruzii podniknuty dva útoky na gruzínské infrastruktury. První byl s nejvyšší pravděpodobností veden ruskými vojenskými silami

156 BASTL 2007 op. cit., s. 47-55.

157 USA např. svěřují kontrolu nad informačními sítěmi ve velké míře armádním složkám, které mají rozsáhlé exekutivní pravomoci. Na druhou stranu existují státy, které akcentují civilní povahu internetu a armádě pravomoci při dohledu nad bezpečností nesvěřují.
O'CONNELL, Marry Ellen. *Cyber Security without Cyber War. Journal of Conflict and Security Law* [online]. 2012, roč. 17, č. 2, s. 187-209 [cit. 16. 8. 2012]. ISSN 1467-7962. Dostupné z: http://jcsl.oxfordjournals.org.

158 Viz již zmíněný počítačový červ Stuxnet popsaný podrobněji dále v tomto textu.

159 O diskuzi zda-li má kybernetický útok povahu zakázaného použití síly či prohibited intervention.
Viz WAXMAN, Matthew. *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4). Yale Journal of International Law* [online]. 2011, roč. 36, č. 2, s. 421-459 [cit. 16. 8. 2012]. Dostupné z: http://heinonline.org.
Dále také BUCHAN, Russell. *Cyber Attacks: Unlawful Use of Force or Prohibited Intervention. Journal of Conflict and Security law* [online]. 2012, roč. 17, č. 2, s. 211-227 [cit. 16. 8. 2012]. ISSN 1467-7962. Dostupné z: http://jcsl.oxfordjournals.org.

160 Někteří již mluví o statistické jistotě, že se obchodní společnost stane terčem nějakého kybernetického útoku, viz LENNON, Mika. *Threat from Cyber Attacks Nearing Statistical Certainty.* SecurityWeek.com [online]. 2011 [cit. 23. 2. 2013]. Dostupné z: http://www.securityweek.com/threat-cyber-attacks--nearing-statistical-certainty.
Nárůst počtu i závažnosti útoků zmiňuje jako jednu z realit bezpečnostní situace současné společnosti i Shackelford, SHACKELFORD, Scott J. *Estonia Two-and-a-Half-Years Later: A Progress Report on Combating Cyber Attacks* [online]. 2009 [cit. 16. 8. 2012]. 12 s. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849. S. 1.

161 RICHMOND, Riva. *Malware Hits Computerized Industrial Equipment.* NYTimes.com [online]. 2010 [cit. 22. 2. 2013]. Dostupné z: http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/.

162 WEISS, Gus W. *The Farewell Dossier: Duping the Soviets* [online]. 2007 [cit. 20. 2. 2013]. Dostupné z: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.
MARKOFF, John. *Old Tricks Threatens the Newest Weapons.* NYTimes.com [online]. 2009 [cit. 20. 2. 2013]. Dostupné z: http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all&.
War in the fifth domain. Economist.com [online]. 2010 [cit. 1. 3. 2013]. Dostupné z: http://www.economist.com/node/16478792.

163 Podrobný popis DAVIS, Joshua. *Hackers Take Down the Most Wired Country in Europe.* Wired.com [online]. 2007 [cit. 23. 2. 2013]. Dostupné z: http://www.wired.com/politics/security/magazine/15-09/ff_estonia.
Dále také TIKK op. cit. 2010, s. 14-36, s. 107.

164 Sdělení Ministerstva zahraničních věcí č. 66/1999 Sb., o přístupu České republiky k Severoatlantické smlouvě. In: CODEXIS [právní informační systém]. Atlas Consulting [cit. 23. 2. 2013].

165 SHACKELFORD 2009 op. cit., s. 5.

166 Stránky na https://www.ccdcoe.org/.

v koordinaci s konvenční vojenskou operací, druhý pak proruskými civilními aktivisty. I tomuto útoku náleží jeden primát, kdy je označován jako první válečná operace zahrnující jak masivní kybernetický útok, tak i konvenční útok plného rozsahu – tedy útok vedený na čtyřech frontách, zahrnujících tři konvenční (země, moře, vzduch) a jednu nekonvenční (kyberprostor).[167] Dříve téhož roku se obětí rozsáhlého mezinárodního kybernetického útoku stala i Litva, kdy bylo na vrcholu útoku zasaženo až 300 webů.[168] Stejně jako v případě Estonska i zde za vším pravděpodobně stála ruská vláda či ruští provládní hackeři,[169] testující schopnost členských států NATO (a potažmo i NATO jako celku) vést informační či kybernetickou válku velkého rozsahu.[170]

Závažné kybernetické útoky se ale dějí i v rámci operací menšího rozsahu jako jsou cílené útoky na infrastruktury či špionáž. Z první kategorie byl zásadním milníkem počítačový červ Stuxnet.[171] Jeho původ v USA či v Izraeli je dnes již jistý a červ byl zaměřen na vyřazení íránských odstředivek na obohacování uranu.[172] Jednalo se o velice sofistikovaný nástroj, který nejenom, že byl maximálním způsobem cílen, ale je prokázáno i využití bezprecedentního množství tzv. *zero exploitů*[173] v jeho kódu. V rámci kybernetické špionáže se pak nechvalně proslulým stal malware Red October, který naopak představoval maximálně sofistikovaný nástroj pro infekci vládních, diplomatických a výzkumných počítačů za účelem získávání tajných či jinak cenných informací.[174]

Zatímco Stuxnet je označován za cílenou zbraň nové generace,[175] Red October bývá označován za špionážní nástroj nové generace.[176] Špionáž velice intenzivně probíhá hlavně ze strany Číny, kdy dochází k rozsáhlým krádežím technologií vyvinutých USA.[177] I vzhledem k esenciální roli výzkumu a vývoje pro moderní společnost a její ekonomiku jsou tedy krádeže spojené s případným zničením kopií zásadním problémem,[178] který představuje jeden z důležitých důvodů pro zajištění kybernetické bezpečnosti.

V posledních letech je také poměrně značným způsobem na vzestupu tzv. hacktivismus, tedy již zmíněná aktivistická činnost hackerů. Využití tohoto prostoru pro apely a protesty je zcela pochopitelné, vzhledem ke značnému mediálnímu prostoru poskytovanému kybernetickým útokům. V této oblasti se vyjímá zejména činnost nehierarchicky uspořádaného hnutí Anonymous, které svými metodami hájilo v minulosti např. Wikileaks nebo naopak napadlo Sony jako reakci na jejich právní kroky vůči komunitě jailbreakerů.[179] Rozsáhlou hackerskou činností se podíleli také na Arabském jaře, kdy napadali prorežimní servery v Tunisku a bojovali proti cenzuře. Stejný postup zopakovali i při událostech v Egyptě, kdy dlouhodobě napadali provládní servery a drželi je mimo provoz až do odstoupení Husního Mubáraka.[180] Zvláštností Anonymous je jejich pouze velmi volné spojení a absence jakékoli hierarchie, což se projevilo např. v průběhu občanské války v Libyi, kdy malá skupina z řad Anonymous působila provládně a útočila na servery opozice.

Hacktivistická činnost se vyskytuje také jako občanská neposlušnost v kyberprostoru za účelem zajištění některých distributivních práv. V rámci dříve v této práci zmíněného katalogu se vyskytuje i právo na informace veřejné správy, v případě odepření pak bývají k jejich získání využity i kybernetické útoky, jako se např. stalo v Lotyšsku na počátku roku 2010, kdy hackeři stáhli značné množství daňových přiznání. S jejich použitím potom upozorňovali na korupci či jiné přinejmenším kontroverzní činy.[181] O tom, že je hacktivismus jednoznačně na vzestupu, svědčí i některá vyjádření přikládající hacktivistům dokonce většinový podíl na ukradených datech.[182] Účelem samozřejmě může být i odlišná motivace útočníků, kdy hacktivisté většinou jedno-

167 HOLLIS, David. *Cyberwar Case Study: Georgia 2008. Small Wars Journal* [online]. 2011, roč. 7, č. 1, s. 1-10 [cit. 1. 10. 2012]. ISSN 0737-1217. Dostupné z: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf. S. 2.

168 TIKK op. cit. 2010, s. 14-36, s. 53.

169 Otázkou pak je odpovědnost státu, pokud hackery cíleně materiálně podporuje či cvičí, ale ti nejsou součástí hierarchických armádních struktur ani zaměstnanci správních či samosprávných orgánů.

170 SHACKELFORD 2009 op. cit., s. 5.

171 Dopadu tohoto počítačového červa na rovnováhu sil v kyberprostoru a na kybernetickou bezpčenost se věnuje PORCHE, Isaac R. III; SOLLINGER, Jerry M.; MCKAY, Shawn. A *Cyberworm that Knows no Boundaries.*[online]. Santa Monica: RAND Corporation, 2011 [cit. 12. 9. 2012]. 55 s. Dostupné z: http://www.rand.org/pubs/occasional_papers/OP342.html.

172 BANKS, William. *The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber War Draft 9/27/12* [online]. 2012 [cit. 18. 10. 2012]. 30 s. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2160078. S. 2.

173 *Zero exploit* představuje dosud neodhalenou slabinu informačního systému či slabinu sice odhalenou, ale se zatím neexistující softwarovou aktualizací vedoucí k jejímu odstranění.

174 Tímto malwarem se intenzivně zabývala Kasperski Lab, ale získal si i pozornost světových médií.
Kasperski Lab Identifies Operation „Red October", an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide [online]. 2013 [cit. 23. 2. 2013]. Dostupné z: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

175 Společně třeba s bezpilotními průzkumnými a útočnými letouny, kterých se ale zabezpečení systémů také týká. Při nedostatečné úrovni kybernetické bezpečnosti totiž může dojít k převzetí navigačních systémů nepřátelskými silami.

176 GOODIN, Dan. *Why the Red October Malware is the Swiss Army Knife of Espionage.* ArsTechnica.com [online]. 2013 [cit. 20. 2. 2013]. Dostupné z: http://arstechnica.com/security/2013/01/why-red-october-malware-is-the-swiss-army-knife-of-espionage/.

177 V minulosti došlo např. ke krádeži dat v rámci klíčového projektu vývoje letounu F-35.
WORTZEL, Larry M. *China's approach to Cyber Operations: Implications for the United States* [online]. 2010 [cit. 22. 2. 2013]. 11 s. Dostupné z: http://origin.www.uscc.gov/china%E2%80%99s-approach-cyber-operations-implications-united-states. S. 5

178 Již SALOMON 1997 op. cit., s. 187 zmiňuje protesty studentů proti příliš těsným vztahům MIT a Pentagonu. Policie tehdy chránila zejména počítače správy a kartotéky, protože podle Salomona by zničení datových bank a informačních sítí (byť i náhodné) znamenalo *„konec průmyslové civilizace jistěji, než požár alexandrijské knihovny symbolizoval konec říše faraonů."*

179 Odblokování zařízení pro použití neoficiálního softwaru.

180 V médiích např. SOMAIYA, Ravi. *Hackers Shut Down Government Sites.* NYTimes.com [online]. 2011 [cit. 22. 2. 2013]. Dostupné z: http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html?_r=2&.

181 O hacktivismu dále PAGET, François. *White Paper on Hacktivism* [online]. 2012 [cit. 20. 2. 2013]. 34 s. Dostupné z: http://www.mcafee.com/hk/resources/white-papers/wp-hacktivism.pdf.

182 Údaje mluví až o 58% ukradených dat.
2012 Data Breach Investigation Report [online]. Verizon, 2012 [cit. 22. 2. 2013]. 76 s. Dostupné z: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf. S. 17.

značně stojí o publicitu, zatímco kyberkriminalita a její pachatelé se snaží co nejvíce zůstat skryti a zaměřují se na cílené útoky. Kyberkriminalita stojí v současné době za největší částí útoků[183] a zaměřuje se hlavně na krádež citlivých dat. Často se jedná o finanční či zdravotní záznamy, kopírování platebních karet nebo o krádeže hesel, jejichž účelem je poté vlastní obohacení formou využití těchto informací či jejich další prodej zájemcům. Pravděpodobně vůbec největším únikem v historii byl únik dat ze společnosti Sony v dubnu roku 2011. Došlo k odcizení údajů k celkem 77 milionům různých uživatelských účtů v rámci PlayStation Network provozované společnosti Sony.[184]

2.2 Prostředky ochrany

Z hlediska kybernetického útoku je cíl ve zcela zřejmé nevýhodě, protože může jen velmi těžko předvídat, kdy nebo odkud útok může přijít a jakými konkrétními prostředky.[185] Vhodným vyhodnocením rizik a nastavením bezpečnostních standardů a politik se však dá poměrně velkému množství útoků předejít nebo zajistit, aby nenapáchaly škody, které by svým způsobem byly nevratné (např. v podobě ztráty osobních nebo jinak citlivých informací). Také systémy včasné reakce na probíhající útok nebo efektivní metody vyšetřování v digitálním prostředí. Kybernetická bezpečnost se tak dá rozdělit do 3 kroků: prevence; reakce; vyšetření/protiopatření.[186]

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015[187] předpokládá vytvoření efektivní politiky vedoucí k posílení kritických informačních infrastruktur a zapracování bezpečnostních standardů, včetně jejich kontroly a vynucování jejich dodržování (úsek prevence); vybudování vládního pracoviště CERT, které bude součástí systému včasného varování na národní i mezinárodní úrovni, bude zajišťovat monitoring, detekci a navrhování protiopatření na národní úrovni v reálném čase (úsek detekce), a které by mělo navrhovat opatření směřující ke snížení následků a neopakování stejných útoků (úsek vyšetření či protiopatření). S poslední složkou kybernetické bezpečnosti samozřejmě souvisí i průběžně se zvyšující schopnost orgánů činných v trestním řízení reagovat na technologický vývoj.

Stejně přistupují k zajištění kybernetické bezpečnosti i strategické koncepce ostatních států. V rámci americké *The National Strategy to Secure Cyberspace*[188] tak Ministerstvo národní bezpečnosti dostává za úkol vytvoření národního plánu identifikujícího kritické infrastruktury a zajišťujícího jejich zabezpečení (prevence); zajištění krizového managementu v reakci na útoky na kritické informační infrastruktury (reakce); výzkum vedoucí k efektivnějším prostředkům ochrany a poskytnutí technických kapacit k nápravě následků kybernetických útoků a uvedení do provozu.[189]

Akty exekutivy ani legislativy, včetně budoucího Zákona o kybernetické bezpečnosti, nesměřují a nesmí směřovat k vyčerpávajícímu soupisu veškerých, při zajišťování kybernetické bezpečnosti použitelných, hardwarových a softwarových nástrojů. Prioritizace některých soutěžitelů na poli informačních technologií prostřednictvím doporučování jejich produktů pro zabezpečení informačních sítí by byla v rozporu jak s národní, tak i s unijní soutěžní legislativou. Přísná technologická neutralita zákona i aktů exekutivy tedy musí být zajištěna na všech úrovních (samozřejmě s výjimkou veřejných zakázek, které již určují konkrétní použité produkty pro konkrétní potřeby veřejné správy a jako takové musí při finálním výběru přistoupit k výběru konkrétní dostupné technologie). Doporučování jednotlivých produktů nebo postupů se tak musí odehrávat pouze v rovině nestranné evaluace a standardizace vedoucí k žádoucímu výsledku, nikoli předepisováním konkrétních systémů či nástrojů, které mají být užity.

Dá se tedy shrnout, že základní metodou k zajištění kybernetické bezpečnosti ze strany státu, a zároveň i jeho základní povinností, je tvorba národní strategie obsahující jasné politiky a cíle, kterých hodlá stát na tomto úseku dosáhnout.[190] Zároveň s vypracováním této strategie je nutné specifikovat kritické informační infrastruktury, které musí být chráněny jako zásadní pro zachování funkčnosti státu a také vypracování bezpečnostního plánu na úrovni exekutivy, které bude specifikovat odpovědnosti jednotlivých orgánů státu. Nezbytnou je rovněž průběžně aktualizovaná analýza rizik. Stejně jako může dojít k tzv. podpojištění nemovitosti, může dojít i při neaktuální analýze rizik k nedostatečnému zabezpečení systému. Ten se může během krátkého času rapidně rozrůst nebo může vzrůst jeho důležitost. K této situaci může dojít i přes to, že by byl původně zabezpečen adekvátním způsobem.

Při vytváření těchto dokumentů se nesmí jednat pouze o izolovanou snahu na úrovni parlamentu či vlády. Důležitá je rovněž celospolečenská diskuze, protože

183 Až 83% zmiňuje 2012 Data Breach op. cit., s. 33.

184 V médiích např. BAKER, Liana B.; FINKLE, Jim. *Sony PlayStation suffers massive data breach*. Reuters.com [online]. 2011 [cit. 23. 2. 2013]. Dostupné z: http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

185 Vše je ještě umocněné extrémní náročností (možná až faktickou nemožností) regulace prostředků, kterými lze provést kybernetický útok. GEERS, Kenneth. *Strategic Cyber Security* [online]. Tallinn: CCD COE Publication, 2011 [cit. 15. 9. 2012]. 168 s. ISBN 978-9949-9040-7-5. Dostupné z: http://www.ccdcoe.org/278.html. S. 123-131.

186 S tím, že třetí krok nás buď vyvede mimo samotnou kybernetickou bezpečnost (tedy do sféry činnosti orgánů činných v trestním řízení) nebo zpět do prevence (přizpůsobení systému aktuální hrozbě). Proto je možné pracovat přímo při zabezpečení kybernetické bezpečnosti pouze se dvěma kroky. *Défense et sécurité des systèmes d'information: Stratégie de la France* [online]. Paris: ANSSI, 2011 [cit. 7. 10. 2012]. 22 s. Dostupné z: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf. S. 15.

187 *Usnesení Vlády České republiky č. 564 ze dne 20. 7. 2011, o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011-2015* [online]. 2012 [cit. 11. 3. 2013]. Dostupné z:http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/5255FA315F9C1833C12578D90031ED95/$FILE/564%20uv110720.0564.pdf.

188 *The National Strategy to Secure Cyberspace* [online]. Washington: The White House, 2003 [cit. 12. 9. 2012]. 60 s. Dostupné z: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

189 National Strategy 2003 op. cit., s. 10-11.

190 *OECD Ministerial Background Report DSTI/ICCP/Reg(2007)/20/FINAL Development of Policies for Protection of Critical Information Infrastructure* [online]. 2007 [cit. 9. 12. 2012]. 101 s. Dostupné z: www.oecd.org/dataoecd/25/10/40761118.pdf.

národní strategie ovlivní i fungování justice nebo soukromého sektoru. Legislativní pokrytí tohoto odvětví je taktéž žádoucí, protože umožní vládě zákonně formulovat a financovat národní program kybernetické bezpečnosti, definovat institucionální rámec pro její zajištění, definovat právní a operační základ pro činnost národních dohledových orgánů a snadnější vstup do unifikačních snah mezinárodního společenství.[191]

Zřejmě nejklíčovějším aspektem kybernetické ochrany jsou pak v současné době týmy CERT,[192] které představují týmy navzájem spolupracujících počítačových bezpečnostních odborníků. Tyto týmy spolupracují jak spolu navzájem, tak s internetovou komunitou a poskytují varování před bezpečnostními hrozbami. Rozlišuje se mezi vládními CERTy, které jsou nadané exekutivními pravomocemi, národními CERTy, který slouží široké veřejnosti a dalšími partikulárními CERT týmy, které slouží konkrétním institucím a spravují bezpečnost jejich sítě.[193] V České republice momentálně působí týmy kooperující na půdě pracovní skupiny CSIRT.CZ, která je koordinovaná sdružením CZ.NIC. Podpisem Memoranda o CERT České republiky[194] došlo k dohodě Ministerstva vnitra a sdružení CZ.NIC, kterým sdružení CZ.NIC převzalo agendu národního CERTu České republiky. Podílí se tak na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice, poskytují koordinovanou pomoc koncovým uživatelům, shromažďují a vyhodnocují data o oznámených incidentech. Jak již bylo zmíněno, nezanedbatelná je edukace v rámci kybernetické bezpečnosti, na které se národní CERT také podílí. Toto pracoviště plnilo do 30. června 2012 také roli vládního pracoviště CERT České republiky. V současnosti je gestorem pro tuto oblasti Národní bezpečnostní úřad, který má za úkol vybudovat do roku 2015 plně funkční Národní centrum kybernetické bezpečnosti jako vládní CERT.

K popisu kompletního a účinného legislativního rámce je dle NATO možné konstatovat existenci několika pravidel, která se dají označit za obecně platná a koherentní s výše uvedeným. Jedná se o teritorialitu, odpovědnost, spolupráci, sebeobranu, ochranu dat, řádnou péči, včasnou výstrahu, přístup k informacím, kriminalizaci a jasný mandát.[195]

Teritorialita představuje suverenitu státu ve vztahu k vlastní kritické infrastruktuře a její ochraně. Nelze tedy, ani při případné existenci unifikovaných mezinárodních aktivit, spoléhat na cizí moc při zajištění kybernetické bezpečnosti. Beze zbytku se jedná o povinnost státu zajistit bezpečnost v zájmu ochrany distributivních práv vlastních občanů. Zároveň se jedná i o zachování suverenity jako takové. S teritorialitou úzce souvisí odpovědnost. Pokud by byl jakýkoli útok prokazatelně spuštěn z informační sítě náležející státu, měl by být tomuto státu i přičitatelný – stát by tedy byl odpovědný za použití vlastní informační sítě náležitým způsobem. Takový stát by měl pomoci s případným vyšetřením incidentu a hledáním opravdových viníků. Toto však v současné době představuje spíše nedosažitelný ideál, kdy není ani jasné, jaký standard pro přičitatelnost jednání v rámci mezinárodního práva vlastně použít.[196]

Navazujícím pravidlem je odpovídající míra spolupráce. Pokud byl z informačních sítí státu veden útok na stát jiný, existuje nejenom odpovědnost, ale zároveň i povinnost asistovat poškozenému při napravování a odhalování škod. Pravidlo sebeobrany, umožňující tzv. *hack-back*, funguje jako *ultima ratio* v případě kybernetického útoku. Zásadním je pak ochrana dat, která ještě jednou akcentuje nutnost chránit osobní údaje uživatelů a znemožňuje i v rámci mezinárodní spolupráce a ohlašovací povinnosti dávat k dispozici veškerá data. Pravidlo řádné péče stanovuje, že každý provozovatel sítě má povinnost implementovat přiměřené obranné mechanismy a pravidlo včasné výstrahy pak zavazuje provozovatele hlásit bezpečnostní incidenty nebo jejich případná rizika. Obě tato pravidla představují zcela zásadní nástroj ochrany. Již zmíněný *cost-effective* přístup soukromého sektoru občas vede k zanedbání kybernetické bezpečnosti. V případě, že pak již nějaký incident nastane, provozovatel může mít tendenci ho zamaskovat, aby udržel důvěryhodnost a zabránil případnému odlivu zákazníků. S tímto přirozeným tržním mechanismem se právě pravidlo řádné péče a včasné výstrahy snaží bojovat. Právo na informace veřejné sféry představuje distributivní informační právo a v přístupu NATO i inherentní část zajištění kybernetické bezpečnosti, což úzce souvisí s již zmíněnou edukativní činností.

Pravidlo kriminalizace by mělo zavazovat státy přijmout do svého trestního práva hmotného úpravu, která by jednoznačně kriminalizovala kybernetické útoky. Nejedná se pouze o nutnost potrestání viníků, ale spíše o možnost efektivního vyšetření za účasti kvalifikovaných orgánů činných v trestním řízení. Posledním je pak požadavek jasného mandátu. Jak bylo zmíněno výše, mezinárodní i národní snahy o zajištění kybernetické bezpečnosti se často překrývají. Ideálním řešením by tedy byl konsensus i mezi jednotlivými mezinárodními organizacemi, které prosazují kybernetickou bezpečnost, na terminologii a společných postupech. Kybernetickou bezpečnost ve svých materiálech momentálně akcentuje Evropská unie, která nedávno připravila návrh Směrnice[197], Mezinárodní telekomunikační unie, OSN i NATO, z čehož pramení různá nedorozumění, potažmo i případné konflikty o obsahu doporučených nejlepších opatření.

Další prostředky ochrany před kybernetickými útoky jsou již v gesci jednotlivých systémových admi-

191 ITU Guide 2011 op. cit., s. 48 a s. 74.

192 Computer Emergency Response Team.

193 Např. Masarykova univerzita má vlastní CERT tým.

194 *Memorandum o Computer Security Incident Response Team České republiky* [online]. 2010 [cit. 17. 2. 2013]. Dostupné z: http://csirt.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf.

195 TIKK Ten Rules 2011 op. cit.

196 SHACKELFORD, Scott J.; ANDRES, Richard B. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Georgetown Journal of International Law* [online]. 2011, roč. 42, č. 4, s. 971-1016 [cit. 16. 8. 2012]. ISSN 1550-5200. Dostupné z: http://heinonline.org. S. 984-992.

197 Comm(2013)48, Návrh Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 12. 3. 2013]. Dostupné z: http://eur-lex.europa.eu/.

nistrátorů i jednotlivých uživatelů. Opatrnost při nakládání s hesly šifrování důležité elektronické komunikace, zálohování dat a pravidelné aktualizování a používání antivirových programů je pro většinu populace stále ještě hudbou budoucnosti, přesto je i v této oblasti možné pozorovat jisté pozvolné zlepšení. Autor si troufá tvrdit, že zlepšení je způsobeno edukativní snahou nejrůznějších organizací, ale hlavně zvýšeným mediálním zájmem o tuto problematiku v posledních letech. Ve společnosti vznikla značně zveličená představa, že jakákoli informační síť, včetně celých států se dá paralyzovat jediným kliknutím myši. Dokud bude tato zveličená a až dobrodružná představa přitahovat zájem médií a mít pozitivní vliv na opatrnost koncových uživatelů při nakládání s vlastními daty a bezpečností na informačních sítích, nedá se než kvitovat ji s povděkem.

3. Úprava kybernetické bezpečnosti v jednotlivých zemích

3.1 Kybernetická bezpečnost ve vyspělých zemích

Vzhledem k dřívějšímu nástupu vývoje informačních technologií v zemích na opačné straně Železné opony se zde rychleji rozvíjela informační společnost i s ní související negativní jevy. Dříve se objevila kyberkriminalita a dříve se objevily informační infrastruktury, které svojí povahou mohly být označeny za kritické. Tyto systémy pak bylo nutné náležitým způsobem zabezpečit. Často se však jednalo pouze o snahy omezené na určitou oblast (např. armády) nebo pouze na soukromý sektor. Obrovský náskok na národní úrovni je tedy do značné míry pouze zdánlivý. I zde teprve masivní rozvoj hrozeb a nárůst důležitosti systémů v posledních přibližně dvou dekádách spustil legislativní a exekutivní činnost. Ta na národní úrovni pak vedla ve snahu upravit kybernetickou bezpečnost, popř. zformulovat celistvé národní strategie. Vedoucími státy na poli kybernetické bezpečnosti z hlediska legislativního rámce je Německo, Spojené království a USA.[198] Jedná se zároveň o velice vhodný reprezentativní výběr a to z následujících důvodů: všechny tři země představují členy NATO, jehož snahy hrají na poli kybernetické bezpečnosti poměrně signifikantní úlohu a jsou pro Českou republiku relevantní; všechny státy jsou členy euroatlantické civilizace a tedy velice podobného socio-kulturního kontextu; ve výběru jsou zastoupeny členské i nečlenské státy EU; ve výběru jsou zastoupeny země kontinentální i angloamerické právní kultury; je zastoupen největší obchodní partner České republiky.

18. 10. 2012 představilo Spojené království novou národní bezpečnostní strategii[199], která mimo jiné obsahuje specifikaci hrozeb, které v současnosti nejvíce ohrožují existenci a funkčnost státu. V kategorii zasluhující si nejvyšší prioritu jsou vedle mezinárodních vojenských krizí, terorismu a rozsáhlých přírodních či jiných katastrof i kybernetické útoky.[200] Plán také mimo jiné akcentuje kromě nezávislých útoků (kyberkriminalita, špionáž atp.) i pomocnou roli kyberprostoru v rámci válečného konfliktu či organizace teroristických buněk.[201] Dokument dále zdůrazňuje nezbytnou spolupráci veřejného a soukromého sektoru jako možnou cestu k zamezení nejenom rozsáhlým kybernetickým útokům, ale i každodenním bezpečnostním incidentům. Dalším důležitým dokumentem, který s národní bezpečnostní strategií úzce souvisí je *UK Strategic Defense and Security Review,*[202] kde jsou dále specifikovány některé hrozby, jejich povaha a postupy, které proti nim mají chránit.

Britská strategie kybernetické bezpečnosti měla být původně publikována na jaře 2011,[203] nakonec se jí však veřejnost dočkala až v listopadu téhož roku. Dokument nazvaný *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*[204] prezentuje vizi, podle které mají být v roce 2015 splněny čtyři cíle:[205] schopnost efektivně poskytovat kyberkriminalitu a představovat bezpečný přístav pro e-commerce v celosvětovém měřítku; schopnost chránit se před kybernetickými útoky a ochraňovat své zájmy v kyberprostoru; zformování stabilního prostředí, které může veřejnost využívat bez obav z kybernetických hrozeb a které bude podporovat otevřenost; zajištění dovedností, znalostí a kapacit pro aktivní výkon kybernetické bezpečnosti. Strategie tak zahrnuje vícestupňovou strukturu zajištění bezpečnosti, která zahrnuje jednotlivce, korporace i stát. Jednotlivec si je dle tohoto schématu vědom rizik, která mu v rámci sítě hrozí.[206] Korporace si pak uvědomují hrozby a zároveň jsou schopné analyzovat rizika, která jim reálně hrozí, a nedostatky ve svých systémech. Prostřednictvím svých obchodních partnerů, zájmových sdružení, hospodářských komor a kooperace se stáními orgány pak pracují na jejich odstraňování. Aktivita soukromého sektoru představuje i ve Spojeném království úhelný kámen jakýchkoli snah směřujících k zajištění kybernetické bezpečnosti, jelikož i zde je většina kritických informačních infrastruktur v soukromých rukou.[207] Za hlavní úkoly státu je pak považováno zefektivnění

198 Zajímavým nástrojem je interaktivní Cyber Power Index dostupný na http://www.cyberhub.com/CyberPowerIndex [cit. 27. 2. 2013]. Při nastavení závažnosti kategorie *„Legal and Regulatory Framework"* na 100% dostáváme právě zmíněné pořadí.

199 *A Strong Britain in the Age of Uncertainty: The National Security Strategy* [online]. London: 2010 [cit. 20. 2. 2013]. 39 s. ISBN 9780101795326. Dostupné z: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.

200 Tamtéž, s. 28-31.

201 Tamtéž, s. 30.

202 *Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review* [online]. London: 2010 [cit. 20. 2. 2013]. 75 s. ISBN 9780101794824. Dostupné z: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf.

203 Tamtéž, s. 49.

204 *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* [online]. London: 2011 [cit. 20. 2. 2013]. 43 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

205 Tamtéž, s. 8.

206 Tedy byl cílem edukační činnosti, která je již dříve v rámci tohoto textu zmíněna jako esenciální pro zajištění kybernetické bezpečnosti „odspodu."

207 UK Cyber Security Strategy 2011 op. cit., s. 8.

práce orgánů činných v trestních řízení na úseku kybernetické bezpečnosti, dále podpora jednotlivců a korporací v jejich činnostech směřujících k potlačení vlastní zranitelnosti,[208] posílení mezinárodní i vnitrostátní spolupráce, efektivní komunikace hrozeb veřejnosti,[209] stimulace soukromého sektoru k zavádění bezpečnostních standardů[210] atd.

Jelikož je tato strategie již nějakou dobu implementována, je možné dohledat i reporty o stavu implementace a shrnutí dosavadní činnosti[211] či prohlášení směřující k dalšímu směřování implementace.[212] Za účelem ochrany informačních sítí vznikl na Ministerstvu obrany nový útvar, Defence Cyber Operations Group, který se má specializovat na vývoj a výzkum nových taktických a operačních postupů v oblasti vojenské kybernetiky, která má v britských podmínkách zahrnovat i prostředky na výše zmíněný *hack-back*.[213] V zemi dále funguje 17 různých CERT týmů,[214] kdy úlohu vládního CERTu plní GovCertUK. I když se i ve Spojeném království hovoří o vytvoření zákona o kybernetické bezpečnosti,[215] zdá se, že exekutivní dokumenty a podpůrná legislativa[216] zcela postačují a samostatný zákon tak zatím, zdá se, není nutností.

Spojené státy se na kybernetickou bezpečnost zaměřují dlouhodobě, jelikož se jedná o vedoucí hi-tech ekonomiku světa. USA mají zároveň zřejmě nejmodernější armádu a vzhledem k její značné aktivitě při mezinárodních operacích je zabezpečení vojenských systémů a zajištění komunikace s vlastním územím kriticky důležité.[217] V rámci národní bezpečnostní strategie z května 2010 zaujímají kybernetické hrozby podobně výsadní postavení jako v rámci strategie britské. Kybernetické hrozby jsou akcentovány zejména v kontextu současného světového bezpečnostního vývoje směrem k již zmíněným asymetrickým konfliktům.[218]

Přístup k informačním sítím, zajišťování jejich bezpečnosti a zajišťování bezpečnosti informací v nich obsažených je předmětem zájmu *Cyberspace Policy Review* z roku 2009,[219] kterým si administrativa stanovila deset krátkodobých cílů mezi kterými byla např. i stále se opakující edukativní činnost.[220] Zároveň bylo stanoveno i čtrnáct střednědobých cílů,[221] které ale na rozdíl od deseti krátkodobých splněny ještě nebyly.[222] Dokument jako takový pak stojí na několika pilířích: zaměřuje se na budování kybernetické bezpečnosti „shora",[223] tedy s náležitou pozorností ze strany nejvyšších míst administrativy, včetně úřadu prezidenta; budování kapacit pro tzv. digital nation, což představuje schopnost jednotlivců v rámci státu uvědomovat si nebezpečí, ale zároveň se účastnit určitých opatření v rámci rozsáhlého ohrožení státu;[224] vybudování principu sdílené bezpečnosti za kybernetickou odpovědnost formou spolupráce s korporátním sektorem;[225] vytvoření platforem pro nahlašování incidentů a sdílení informací o kybernetických útocích a bezpečnostních incidentech;[226] a konečně posílení inovací v rámci kybernetické bezpečnosti.[227]

Unikátním podnikem je pak v dubnu 2011 představená strategie *National Strategy for Trusted Identities in Cyberspace*.[228] Strategie směřuje k vytvoření online

208 Ve vztahu ke korporátnímu sektoru se jedná zejména o následující dokumenty:
10 Steps to Cyber Security [online]. London: The Information Security Arm of GCHQ, 2012 [cit. 20. 2. 2013]. 22 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73129/12-1121-10-steps-to-cyber-security-advice-sheets.pdf.
10 Steps to Cyber Security: Executive Companion [online]. London: The Information Security Arm of GCHQ, 2012 [cit. 20. 2. 2013]. 20 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf.

209 V tomto směru je obzvláště důležitá britská platforma GetSafeOnline.org.

210 Jako poradenské centrum v této oblasti funguje funguje Center for Protection of National Infrastructure (domovská stránka na http://www.cpni.gov.uk/). V rámci CPNI pak existují kontaktní místa pro nahlašování incidentů a sdílení informací pro specifická odvětví (např. Transport Sector Information Exchange a Aerospace and Defence Manufacturer's Information Exchange). *United Kingdom Country Report* [online]. ENISA, 2011 [cit. 20. 2. 2013]. 52 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/UK.pdf. S. 16-17.

211 *Progress Against the Objectives of the National Cyber Security Strategy – December 2012* [online]. 2012 [cit. 20. 2. 2013]. 6 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf.

212 *The UK Cyber Security Strategy Report on Progress December 2012 – Forward Plans* [online]. 2012 [cit. 20. 2. 2013]. 9 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83757/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf.

213 GARDHAM, Duncan. *Britain Prepares for Cyber War*. Telegraph.co.uk [online]. 2011 [cit. 25. 2. 2013]. Dostupné z: http://www.telegraph.co.uk/news/uknews/defence/8915871/Britain-prepares-for-cyber-war.html.

214 UK ENISA 2011 op. cit., s. 13.

215 CLEMENTE, Dave. *Defence and Cyber-security: Written Evidence* [online]. 2012 [cit. 25. 2. 2013]. Dostupné z: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm.

216 Zejména se jedná o Computer Misuse Act of 1990, Data Protection Act 1998, Electronic Communications Act of 2000, Electronic Signatures Regulation 2002, Civil Contingencies Act 2004, kterými se samozřejmě implementovaly příslušné předpisy EU.

217 Důležitost, která je kladena informační bezpečnosti v americké armádě je možné ilustrovat na publikaci *Information Operations Primer: Fundamentals of Information Operations*, která je opakovaně aktualizována pro potřeby výuky na US Army War College. Publikace je k dispozici na http://www.carlisle.army.mil/usawc/dmspo/Publications/Information%20Operations%20Primer%20AY12%20Web%20Version.pdf [cit. 1. 3. 2013].

218 *National Security Strategy* [online]. Washington: The White House, 2010 [cit. 27. 2. 2013]. 52 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. S. 17.

219 *Cyberspace Policy Review* [online]. 2009 [cit. 27. 2. 2013]. 76 s. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

220 Tamtéž, s. 37.

221 Tamtéž, s. 38.

222 Věcný záměr 2012 op. cit., s. 41.

223 Cyberspace Policy Review 2009 op. cit., s. 7-11.

224 Tamtéž, s. 13-15.
O tomto aspektu zvyšování kybernetické bezpečnosti země různými metodami je ostatně pojednáváno i v rámci KLIMBURG, Alexander. *The Whole of Nation in Cyberpower. Georgetown Journal of International Affairs* [online]. 2011, zvláštní vydání, s. 171-179 [cit. 16. 8. 2012]. ISSN 1526-0054. Dostupné z: http://heinonline.org.

225 Cyberspace Policy Review 2009 op. cit., s. 17-21.

226 Tamtéž, s. 23-29.

227 Tamtéž, s. 31-35. Všechny tyto jednoduché principy je zároveň možné pozorovat jak v této práci, tak ve Věcném návrhu Zákona o kybernetické bezpečnosti ČR i jako prozařující napříč britským přístupem ke kybernetické bezpečnosti. Představují totiž určitou praxi, která je vnímána jako inherentní jakémukoli efektivnímu systému zajištění kybernetické bezpečnosti.

228 *National Strategy for Trusted Identities in* Cyberspace [online]. Washington: The White House, 2011 [cit. 2. 3. 2013]. 45 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

prostředí příznivého pro uživatele zejména co se týče bezpečnosti jejich identit. Tento tzv. *identity ecosystem*[229] představuje soubor mechanismů směřující k možnosti uživatelů prokázat svoji totožnost pomocí prezentace pouze těch údajů o uživateli, které jsou relevantní pro uskutečnění transakce nebo přístup k danému obsahu. Nesdílením masy osobních údajů, ale pouze relevantního segmentu, se také limituje riziko krádeže identity a zneužití těchto údajů pro kriminální činnost. Nejedná se o koncept nový, zmiňoval ho již Lawrence Lessig.[230] Nicméně snaha USA v této oblasti představuje premiérový plán na prosazení v praxi.

V květnu 2011 pak byla zveřejněna *International Strategy for Cyberspace*,[231] která představuje celistvou strategii v přístupu ke kyberprostoru a integruje ji do jednotlivých aspektů americké administrativy. Kybernetická bezpečnost v rámci tohoto dokumentu směřuje hlavně k zabezpečení kritických informačních infrastruktur, posílení mezinárodní bezpečnosti a zlepšení schopnosti odpovědět a náležitě reagovat na kybernetické útoky a kyberkriminalitu. K tomu má docházet zejména akcentací vhodné regulace, ale také vojenskou i civilní spoluprací se spojenci. Výhradní dohled nad civilními sítěmi má dle americké legislativy *Department of Homeland Security*, které ale poměrně úzce spolupracuje s dohledovým orgánem pro sítě vojenské, kterým je *US Cyber Command*. To představuje jednotné kybernetické velitelství pro všechny vojenské složky a akcentuje tak úlohu kyberprostoru ve vojenské doktríně USA jako separátní operační domény ve vedení války.[232] Z hlediska kybernetické bezpečnosti má výsadní postavení dokument Ministerstva obrany z června 2011 nazvaný *Department of Defense Strategy for Operating Cyberspace*.[233] Klíč k zabránění útoku (či spíše k minimalizaci pravděpodobnosti jeho úspěšného uskutečnění) je postavený na pěti pilířích: posílení role kyberprostoru jako již zmíněné páté operační domény;[234] kladení důrazu na aktivní obranu[235] např. formou detekce škodlivého kódu a jeho analýzy;[236] ochraně kritické infrastruktury[237] (zařazuje finanční sektor, přenosovou soustavu a transportní systémy); vytvoření mezinárodní ochrany před kybernetickými útoky jak v rámci struktur NATO, tak i nezávisle na nich v rámci trvalých (či případných *ad hoc*) spojeneckých vztahů;[238] a konečně výzkum a výcvik na poli kybernetické bezpečnosti.[239] Na druhou stranu tato strategie neodpověděla na dlouho diskutovanou otázku možnosti konvenční odpovědi na kybernetický útok. Předpokládá se, že tuto otázku řeší část strategie podléhající utajení. Dalším dokumentem, který by měl obsahovat tzv. *rules of engagement* řešící možnost aktivní kybernetické obrany nebo nasazení konvenčních sil je utajená *Presidential Policy Directive 20*.[240] USA mají samozřejmě řadu CERT týmů, kdy nejdůležitějším je US-CERT, který je hlavním národním týmem zodpovědným za okamžitou reakci v otázkách narušení kybernetické bezpečnosti.

Stejně jako ve Spojeném království ani v USA momentálně neexistuje legislativní zakotvení kybernetické bezpečnosti. Zatím posledním dokumentem směřujícím k celistvé legislativě upravující kybernetickou bezpečnost byl *Cybersecurity Act* z roku 2012,[241] kterému vyjádřil velice silnou podporu prezident Barack Obama, ale který byl nakonec stejně legislativci *de facto* smeten ze stolu.[242] Problémem byla mimo jiné i silná opozice ze strany jak korporací, tak i organizací hájících práva uživatelů. První ze jmenovaných skupin se obávala tíživého ekonomického dopadu navržených opatření v průběhu ekonomické krize. Návrh sice pracoval s dobrovolným zavedením bezpečnostních standardů, hospodářská komora se ale obávala postupné novelizace předpisu a zavedení standardů povinných.[243] Druhou ze skupin pak zastupovala hlavně známá a vlivná organizace *Electronic Frontier Foundation*, která se obávala hlavně excesivního sledování uživatelů webových stránek a obecně všech služeb informační společnosti.[244] Příliš široce nastavený mandát umožňující korporacím sdílet osobní údaje uživatelů jejich systémů s ostatními korporacemi i s vládou,[245] pokud je předmětem zajištění

Webové stránky je možné nalézt na http://www.nist.gov/nstic/ [12. 3. 2013].

229 Tamtéž, s. 21-27.

230 LESSIG, Lawrence. *Code: version 2.0* [online]. New York: Basic Books, 2006 [cit. 9. 12. 2012]. 410 s. ISBN 0465039146. Dostupné z: http://codev2.cc/download+remix/Lessig-Codev2.pdf. S. 51.

231 *International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World* [online]. Washington: The White House, 2011 [cit. 3. 3. 2013]. 25 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

232 Kyberprostor se tak přidal k zemi, moři, vzduchu a vesmíru. *Department of Defense Strategy for Operating in Cyberspace* [online]. 2011 [cit. 1. 3. 2013]. 19 s. Dostupné z: http://www.defense.gov/news/d20110714cyber.pdf. S.5.

233 Tamtéž.

234 Tamtéž, s. 5-6.

235 Tamtéž, s. 6-7.

236 V úvahu by zde teoreticky mohlo připadat i použití tzv. honeypotů pro studium nových metod kybernetického útoku či kontrolované simulované průniky do systémů ze strany specializovaných skupin v rámci armádní hierarchie. Případný *hack-back* by také spadal do této kategorie.

237 DoD Strategy 2011 op. cit., s. 8-9.

238 Tamtéž, s. 9-10.

239 Tamtéž, s. 10-12.

240 Předpokládá se, že specifikuje rozdíly mezi obranným a útočným použitím kybernetických sil a metod kybernetického boje, specifikuje stupně ohrožení, které spustí případnou vojenskou odezvu atp. Přesný obsah však zůstává vzhledem ke stupni utajení veřejnosti neznámý.
Viz NAKASHIMA, Ellen. *Obama signs secret directive to help thwart cyberattacks.* WashingtonPost.com [online]. 2012 [cit. 9. 3. 2013]. Dostupné z: http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense.

241 *A Bill: Cybersecurity Act of 2012*. In: GovTrack.us [nástroj zpřístupňování veřejné moci]. Civic Impulse [cit. 4. 3. 2013]. Dostupné z: http://www.govtrack.us/.

242 COUTS, Andrew. *Senate Kills Cybersecurity Act of 2012.* DigitalTrends.com [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/.

243 EGGERS, Matthew. *Enough With the Distractions … It's Time for Consensus-Oriented Cybersecurity Legislation.* FreeEnterprise.com [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: http://www.freeenterprise.com/enough-distractions-it-s-time-consensus-oriented-cybersecurity-legislation.

244 REITMAN, Rainey. *New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities* [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities.

245 Tato připomínka se týká zejména v lednu 2013 představeného návrhu nového zákona.
Viz *A Bill: Cyber Intelligence Sharing and Protection Act*. In: GovTrack.us [nástroj zpřístupňování veřejné moci]. Civic Impulse [cit. 4.3. 2013]. Dostupné z: http://www.govtrack.us/.

kybernetické bezpečnosti, je tak permanentním bodem rozsáhlých diskuzí. Tato otázka je zejména po excesech NSA na úseku sledování telekomunikačních provozu po událostech 11. 9. 2001, které vyvrcholily zveřejněním existence programu PRISM, ve středu pozornosti nejen americké veřejnosti a zájmových skupin. K jakýmkoli obavám se pak ještě přidává dobře známý aktivistický přístup administrativy USA k vynucování si dodržování práv duševního vlastnictví, který ukazuje, že by obavy nemusely být pouze paranoidního charakteru, ale mohly mít i reálný základ.

V Německu je v současné době také věnována kybernetické bezpečnosti značná pozornost a Německo je jedním ze států, které se účastní na činnosti již zmíněného Centra excelence v Tallinnu.[246] Národní strategie pochází z února 2011[247] a celá je založena na činnosti dvou základních orgánů – Centra pro kybernetickou obranu[248] a Radě kybernetické bezpečnosti.[249] Tým Centra pro kybernetickou ochranu tvoří šest zástupců Spolkového úřadu informační bezpečnosti, dva zástupci Spolkového úřadu pro ochranu ústavy a Spolkového úřadu pro ochranu obyvatelstva a pomoc při živelných katastrofách. Počítá se s účastí hostujících expertů z kriminální policie, armády, zpravodajských služeb či celních úřadů k zajištění maximální efektivity jakýchkoli postupů. Strategie je bohužel velmi vágní při stanovení jakýchkoli pravomocí či předpokládaných výstupů činnosti centra.[250]

Rada kybernetické bezpečnosti pak má představovat vrcholný orgán se zástupci ze všech relevantních spolkových ministerstev, kteří mají řešit závažná celonárodní ohrožení kritické informační infrastruktury. Dalším pilířem kybernetické bezpečnosti je podle německé strategie výzkum a vývoj na poli kybernetické bezpečnosti a zajištění nejenom technologické neutrality, ale i rozmanitosti používaných technologií k zajištění maximální spolehlivosti.[251] Strategie zároveň zmiňuje koncepci udržitelné implementace, která zohledňuje krátkou životnost jakýchkoli implementovaných opatření tváří v tvář rapidně se vyvíjejícím a měnícím kybernetickým hrozbám.[252] Je tedy třeba neustálá periodická revize zavedených opatření tak, aby nezastarala a byla stále efektivní. Již zmíněný Spolkový úřad informační bezpečnosti zároveň představuje komunikační platformu pro nahlašování kybernetických útoků a pro sdílení informací o nebezpečích. Jednou za dva roky pak také publikuje zprávu o bezpečnosti informačních technologií v Německu.[253]

Součástí německého snažení o zajištění kybernetické bezpečnosti jsou i organizované vzdělávací akce a akce s účelem zvýšení povědomí veřejnosti o aktuálních aspektech kybernetické bezpečnosti. Nutnost edukace ostatně zmiňuje i implementační plán pro zajištění bezpečnosti kritických informačních infrastruktur,[254] který představuje základní dokument pro dlouhodobé partnerství a spolupráci veřejného a soukromého sektoru. Na plnění plánu dohlíží čtyři pracovní skupiny, které mají v čele zástupce soukromého sektoru – jedná se o skupinu pro pohotovostní a krizová cvičení; krizové řízení a reakci; udržování služeb kritických infrastruktur; skupinu pro národní a mezinárodní spolupráci.[255] V Německu v současné době funguje více než 50 různých CERT týmů[256] a roli vládního týmu plní CERT-BUND. K vytvoření vyčerpávající legislativy upravující kybernetickou bezpečnost ani v Německu zatím ještě nedošlo.

Co se týče kybernetické bezpečnosti, dá se tedy konstatovat na úrovni nejvyspělejších států vzácná vzájemná shoda na některých základních aspektech kybernetické bezpečnosti, kterých se všechny tři výše zmíněné státy snaží dosáhnout. Jako základní aspekty kybernetické bezpečnosti můžeme s ohledem na vše výše uvedené označit následující:

- Zformování národní strategie kyberprostoru a národní strategie kybernetické bezpečnosti.
- Jasná specifikace mandátu jednotlivých složek státu v rámci kybernetické bezpečnosti, ať již dojde ke zdůraznění úlohy vojenského či civilního sektoru.
- CERT týmy, které již nepředstavují pouze best-practice aspekt kybernetické ochrany, ale nutnost, a to jak za účelem ochrany soukromých sítí (národní CERT), tak sítí veřejných úřadů a státních orgánů (vládní CERT). Exekutivní pravomoci vládního CERTu mohou být veřejností vnímány kontroverzně, přesto se zdají být vhodným nástrojem pro řešení bezpečnostních incidentů velkého rozsahu (riziko výpadku páteřní sítě atp.).
- V případě efektivního postupu v rámci jiných zákonů není nutná souhrnná zákonná úprava kybernetické bezpečnosti, i když se státy o její alespoň částečnou implementaci dlouhodobě snaží.

Další komentáře je možno nalézt v rámci FAQ organizace EFF na https://www.eff.org/cybersecurity-bill-faq [12. 3. 2013].

246 Kromě Německa se činnosti účastní ještě Litva, Lotyšsko, Estonsko, Nizozemsko, Polsko, Slovensko, Maďarsko, Španělsko a Itálie.

247 *Cyber Security Strategy for Germany* [online]. Berlin: Federal Ministry of the Interior, 2011 [cit. 10. 7. 2012]. 20 s. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

248 Tamtéž, s. 8.

249 Tamtéž, s. 9-10.

250 Věcný záměr 2012 op. cit., s. 34.

251 Strategy for Germany 2011 op. cit., s. 11-12.

V této fázi se dá diskutovat o dalším aspektu kybernetické bezpečnosti, kterým je prevence bezpečnostních a technologických monokultur. Ty mohou zvyšovat zranitelnost systému např. cílenými programovými změnami ve „výrobní" fázi či tzv. kaskádovým selháním, které je právě v technologické monokultuře pro útočníka mnohem snadněji dosažitelné.

GEER, Daniel E. *Cybersecurity and National Policy. Harvard National Security Journal* [online]. 2010, roč. 1, č. 1, s. 203-215 [cit. 12. 9. 2012]. ISSN 2153-1358. Dostupné z: http://www.harvardnsj.com/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf. S. 205-206.

252 Tamtéž, s. 13.

253 Zatím poslední zpráva je z roku 2011.

The IT Security Situation in Germany in 2011 [online]. Bonn: Federal Office for Information Security, 2011 [cit. 4. 3. 2013]. 48 s. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2011_pdf.pdf?__blob=publicationFile.

254 *CIP Implementation Plan of the National Plan for Information Infrastructure Protection* [online]. Federal Ministry of Interior [cit. 4. 3. 2013]. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/UP_KRITIS_en_final.pdf?__blob=publicationFile. S. 24.

255 *Germany Country Report* [online]. ENISA, 2011 [cit. 20. 2. 2013]. 47 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf. S. 26.

256 Jejich seznam je možné nalézt tamtéž, s. 33-44.

- Je nutné vytvořit prostředí, které bude dostatečným způsobem stimulovat a usnadňovat výměnu informací o bezpečnostních incidentech a jejich nahlašování za účelem maximální informovanosti. V případě, že nestačí stimuly, je nutné tuto povinnost zakotvit.
- Edukace veřejnosti hraje v zajišťování kybernetické bezpečnosti klíčovou úlohu, protože nakonec s počítačem vždy manipuluje koncový uživatel.
- Je nezbytné zapojit do kybernetické bezpečnosti (opět formou stimulů či přímo povinnosti) korporátní sektor, protože značná část kritických informačních struktur je v soukromém vlastnictví.
- Technologická neutralita musí být zajištěna.

3.2 Kybernetická bezpečnost ve střední a východní Evropě

Kybernetická bezpečnost má, jak již bylo opakovaně zmiňováno, těžší pozici prosadit se v zemích, které měly v minulosti zkušenost s totalitními režimy. Zásad státu do distributivních práv jednotlivců, za účelem ochrany práv nedistributivních, se často setkává s odporem ze strany občanů i neziskových organizací. Zároveň jsou pak státní správy těchto zemí často stiženy nedostatečnou odborností úředníků, kteří byli dosazeni z politických důvodů. Dalším problémem je také palčivě vnímaný problém korupce, který často téměř automaticky v očích občanů delegitimizuje (a delegalizuje) navržené implementační projekty.

Ze zemí východní a střední Evropy má největší náskok na poli kybernetické bezpečnosti Estonsko. Vzhledem k událostem z roku 2007 si estonská společnost jako celek uvědomila, že zajištění kybernetické bezpečnosti je *conditio sine qua non* fungující informační společnosti v 21. století. Estonská společnost je poměrně unikátní v důrazu, jaký klade na informační systémy – v zemi je možné volit přes internet,[257] má rozsáhlé zdarma dostupné Wi-Fi pokrytí, povinnost podávat některá daňová přiznání elektronicky[258] atd. V roce 2008 byla Ministerstvem obrany představena *Kuberjulgeoleku strateegia*[259] pro roky 2008-2013. Strategie mluví o pěti klíčových politikách: vývoj a nasazení bezpečnostních opatření; zvýšení kompetentnosti; úprava legislativního rámce za účelem zvýšení kybernetické bezpečnost; posílení mezinárodní spolupráce; zvýšení zájmu společnosti.[260] V zemi vzniklo Centrum excelence NATO a dobrovolná organizace Küberkaitseliit[261] a došlo k výraznému propojení soukromého a veřejného sektoru. Dále došlo k nastavení standardů šifrování[262] a k vytvoření zvláštních jednotek pro vyšetřování a stíhání kyberkriminality v rámci policie a celních úřadů. Vše za účelem posílení bezpečnosti koncového uživatele v rapidně se rozvíjející informační společnosti. Národním CERTem je CERT.ee, který zároveň s činností směřující k větší informovanosti a řešení kybernetických incidentů provádí i *reverse engineering* nových škodlivých programů.[263] Legislativní úprava kybernetické bezpečnosti v podobě, v jaké je plánována v ČR, v zemi momentálně neexistuje. I již zmíněná strategie kybernetické bezpečnosti počítá spíše s úpravou formou podpůrné legislativy a novelizací již existujících předpisů, spíše než s vytvořením nové vyčerpávající úpravy.

Situace v dalších dvou pobaltských zemích, v Litvě a v Lotyšsku, je poněkud komplikovanější. Ač se, jak již bylo v textu dříve zmíněno, Litva stala v minulosti cílem útoku velkého rozsahu a oba státy se zároveň účastní činnosti Centra excelence NATO, kybernetická bezpečnost není na takové úrovni jako třeba v Estonsku. Gestorem kybernetické bezpečnosti v Litvě je Ministerstvo vnitra, činnost pak probíhá zejména přes pod něj spadající oddělení informačních a komunikačních technologií. *Program pro rozvoj elektronické informační bezpečnosti (kybernetické bezpečnosti) pro roky 2011 – 2019*[264] sleduje stejně tak jako většina již zmíněných programů několik obecných cílů. Výjimečným je v tomto případě ale zařazení i několika cílů, které je možné kvantifikovat. Do roku 2019 má být dosaženo stavu, kdy se 60% uživatelů cítí v kyberprostoru bezpečně, odezva na bezpečnostní incident v rámci kritické informační infrastruktury má být nejvíce 30 minut a 98% kritické infrastruktury má být zabezpečeno způsobem odpovídajícím vnitrostátní legislativě.[265] Určitého kvalitativně nižšího stavu má být dosaženo již v roce 2015.[266] Celý dokument je dle autora poměrně podivuhodný, právě kvůli kombinaci obecných i kvantifikovatelných cílů. Národním CERTem je CERT-LT, v zemi je ale možné nalézt několik dalších CERT týmů – jedná se zejména o IST-

257 Ve volbách v roce 2011 bylo odevzdáno elektronickou formou celkem 24,3% hlasů.
Obecně *Internet Voting in Estonia* [online]. Vabariigi Valimiskomisjon [cit. 10. 3. 2013]. Dostupné z: http://www.vvk.ee/voting-methods-in-estonia/engindex/.
Viz také §48 a násl., Riigikogu Election Act, ve znění k 11. 11. 2012. In: *LegalText.ee* [anglická znění zákonů]. Justiits ministeerium [cit. 10. 3. 2013]. Dostupné z: https://www.riigiteataja.ee/.

258 *As of 1 January 2009, in some cases, submission of the forms TSD and KMD in electronic format shall be mandatory* [online]. Estonian Tax and Customs Board [cit. 10. 3. 013]. Dostupné z: http://www.emta.ee/index.php?id=25299. V roce 2012 bylo dokonce 94% daňových přiznání k dani z příjmu podáno elektronicky. Další informace o využití informačních technologií v běžném životě v Estonsku je možné nalézt na http://estonia.eu/about-estonia/economy-a-it/e-estonia.html [10. 3. 2013].

259 *Cyber Security Strategy* [online]. Tallinn: Ministry of Defence, 2008 [cit. 10. 3. 2013]. 36 s. Dostupné z: http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf.
Ač původně mělo na starost kybernetickou bezpečnost Ministerstvo obrany, nakonec byla tato kompetence přenesena na Ministerstvo hospodářství a komunikace.

260 Tamtéž, s. 3-5.

261 GJELTEN, Tom. *Volunteer Cyber Army Emerges in Estonia.* NPR.org [online]. 2011 [cit. 10. 3. 2013]. Dostupné z: http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation.

262 Standardně se používá 2048-bitové šifrování pro elektronické občanské průkazy a pro elektronické podpisy.

263 *Estonia Country Report* [online]. ENISA, 2011 [cit. 20. 2. 2013]. 30 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Estonia.pdf. S. 11.

264 *The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019* [online]. Vilnius, 2011 [20. 2. 2013]. 17 s. Dostupné z: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf.

265 Tamtéž, s. 1.

266 Tamtéž, přílohy.

-SVDPT, LITNET CERT a čtyři vojenské CERT týmy úzce spolupracující s CERT-LT.[267] Litva bohužel, i přes snahu zapojovat se do mezinárodních aktivit, představuje téměř pravý opak Estonska. V zemi téměř zcela absentuje spolupráce vládního a soukromého sektoru a povědomí koncových uživatelů o nebezpečích je jen velice vágní, což je odbornou veřejností opakovaně kritizováno.[268] Ve strategii zmiňovaná nutnost edukace je tedy v Litvě absolutní nutností, protože momentálně litevská společnost představuje v této oblasti spíše kulturu strachu.[269] Strategie také konstatuje fragmentovanou úpravu kybernetické bezpečnosti v předpisech nižší než zákonné právní síly jako nedostatečnou.[270] Dá se tedy očekávat, že snaha o zajištění kybernetické bezpečnosti bude v Litvě někdy v nedaleké budoucnosti gradovat podobnými snahami jako v ČR.

Lotyšsko v minulosti přijalo zákon o bezpečnosti informačních technologií.[271] Z působnosti zákona je absolutně vyloučen obsah informací přenášených informačními sítěmi. Zákon také ustavuje CERT.LV jako lotyšský *response team* pro bezpečnostní incidenty a výslovně mu zapovídá možnost žádat jakékoli poplatky za poskytování služeb, které jsou mu předepsány zákonem. CERT.LV organizačně přísluší pod Ministerstvo dopravy a komunikací. Zákon ustavuje, v rámci sítí ve své působnosti, povinnost informovat o bezpečnostním incidentu CERT.LV a zároveň umožňuje takové jednání tam, kde nemá možnost jej přímo nařídit. Lotyšské trestní právo také obsahuje zvláštní skutkovou podstatu porušení bezpečnostních opatření v informačních sítích.[272] Za účelem posílení spolupráce se soukromým sektorem (která, stejně jako v Litvě, ani zdaleka nedosahuje estonského rozsahu) nedávno vznikla iniciativa, sdružující ISP ochotné spolupracovat s CERT.LV na řešení bezpečnostních incidentů.[273] Na první pohled je tedy zřejmé, že Lotyšsku se podařilo vytvořit poměrně silný legislativní rámec pro zajištění kybernetické bezpečnosti. I přes tento stav a edukativní snahy však zůstává veřejnost spíše neinformovaná.

V Maďarsku, stejně jako v jiných zemích, již s kybernetickou bezpečností přímo počítá i národní bezpečnostní strategie.[274] Cílem je zvýšení bezpečnosti kritických informačních infrastruktur a také intenzivní spolupráce na výzkumu a implementaci bezpečnostních opatření společně s EU, NATO a dalšími spojenci.[275] Význam kybernetické bezpečnosti je tedy v Maďarsku akcentován jejím zařazením jako kritického odvětví celostní národní bezpečnosti. Vládním CERTem je CERT-Hungary, který funguje od roku 2010 jako Centrum kybernetické bezpečnosti Maďarska, které spadá pod Úřad předsedy vlády.[276] Úkolem CERTu je koordinační činnost při útocích velkého rozsahu, podpora informační výměny mezi kritickými odvětvími informační společnosti a edukace. Maďarsko je také jedním z participujících států na činnost Centra excelence NATO v Tallinnu. Maďarsko má také k dispozici poměrně unikátní úřad, MIBA, který se zabývá standardizací a certifikací bezpečnostního softwaru a také hodnotí dostupná bezpečnostní opatření na organizační a institucionální úrovni.[277] Určité mezery ve znalostech nejenom veřejnosti, ale i korporátního sektoru, a v opatrnosti jejich chování ve vztahu ke kybernetické bezpečnosti, stále existují. Situace se ale v posledních letech zlepšuje proaktivním přístupem vládního sektor,[278] který vyústil dne 21. 3. 2013 k přijetí Vládního rozhodnutí č. 1139/2013, které specifikuje Národní strategii kybernetické bezpečnosti[279] a dne 15. 4. 2013 k přijetí zákona o kybernetické bezpečnosti ústředních a regionálních úřadů.[280]

Polsko je, i přes svoji účast v Centru excelence NATO v Tallinnu a intenzivní snahu o mezinárodní spolupráci, vnímáno jako země v evropském měřítku málo připravená na kybernetické útoky.[281] Opatření k zajištění kybernetické bezpečnosti jsou často odsouvána nebo nejsou implementována náležitým způsobem.[282] Polsko se vyznačuje poměrně silnou militarizací kyberprostoru a technicky je poměrně solidně vybaveno, nicméně autority často nekladou na kybernetické hrozby podobný důraz jako na hrozby konvenční.[283] Nejdůležitějším dokumentem je v současnosti národní strategie ochrany kyberprostoru,[284] který ale poměrně dlouho čekal na schválení,[285] což dokonale dává za pravdu kritice o nedostatečné pozornosti věnované kybernetické bezpečnosti. Původní verzi dokumenty také byly vytýkány některé chyby, které minimálně zpochybňovaly pozor-

267 *Lithuania Country Report* [online]. ENISA, 2011 [cit. 20. 2. 2013]. 24 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Lithuania.pdf. S. 22.

268 SAPETKAITĖ, Vaiva. *Kibernetinis (ne)saugumas: Baltijos šalių situacija.* Geopolitika.lt [online]. 2012 [cit. 20. 2. 2013]. Dostupné z: http://www.geopolitika.lt/?artc=5504.

269 Tak, jak o ni mluví ve své eseji v souvislosti s kybernetickou bezpečností GEER 2010 op. cit.

270 Development 2011-2019 op. cit., s. 3

271 Zákon je k dispozici na http://www.likumi.lv/doc.php?id=220962 [cit. 20. 2. 2013], kde je k dispozici i jeho anglický překlad.

272 *Latvia Country Report* [online]. ENISA, 2011 [cit. 20. 2. 2013]. 25 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Latvia.pdf/at_download/file. S. 6.

273 Memorandum o připojení k této iniciativě je možné nalézt na http://www.lia.lv/media/uploads/Saprasanas_memorands_informativi.pdf [cit. 10. 3. 2013].

274 *Hungary's National Security Strategy* [online]. Ministry of Foreign Affairs, 2012 [cit. 22. 2. 2013]. 23 s. Dostupné z: http://www.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf.

275 Tamtéž, s. 13-14.

276 Věcný záměr 2012 op. cit., s. 36-37.

277 *Hungary Country Report* [online]. ENISA, 2011 [cit. 16. 10. 2013]. 30 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Hungary.pdf. S. 10.

278 Tamtéž, s. 19.

279 *Hungary's National Cyber Security Strategy of Hungary* [online]. 2013. [cit. 16. 10. 2013]. 7 s. Dostupné z: http://nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx.

280 *Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies* [online]. 2013. [cit. 16. 10. 2013]. Dostupné z: http://nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx

281 ŚWIĄTKOWSKA 2012 op. cit., s. 49-50.

282 Tamtéž, s. 6.

283 Tamtéž.

284 *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* [online]. 2010 [cit. 1. 3. 2013]. 33 s. Dostupné z: http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf.

285 Došlo k němu až v roce 2012.

nost, s jakou byl dokument vytvářen.[286] V zemi dále funguje CERT.GOV.PL, jako centrum technické podpory pro zajištění funkčnosti a rozvoj ochrany sítí státní správy a samosprávných orgánů. Administrativně spadá pod ABW,[287] což je polská obdoba BIS. Polsko se v současné době snaží legislativně zakotvit kybernetickou bezpečnost, protože jakékoli další snahy se zdají být limitovány nedokonalou legislativou.[288] Zajímavý je výskyt kybernetických hrozeb v polské úpravě stanného práva.[289] K vyhlášení stanného práva může dojít i v souvislosti s kybernetickým útokem, stejně tak i k vyhlášení stavu nebezpečí či stavu přírodní katastrofy, pokud není možné nastalou situaci řešit jinými prostředky. K tomuto všemu přispívá také fakt, že Polsko přijalo zákonnou definici kyberprostoru,[290] který je pak přidán k ostatním sférám, kde státní orgány vykonávají svoji svrchovanost.

Slovensko se ve svých snahách poměrně striktně drží terminologie EU a při úpravě kybernetické bezpečnosti používá pojem bezpečnosti informační. *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike*[291] zahrnuje následující strategické priority: otázky ochrany lidských práv a svobod; budování povědomí a kompetentnosti v oblasti informační bezpečnosti; vytváření bezpečného prostředí; zefektivnění řízení informační bezpečnosti; zajištění dostatečně ochrany kritických informačních infrastruktur; mezinárodní a národní spolupráci při řešení bezpečnostních incidentů; zvyšování vlastní kompetentnosti. Mezi další cíle slovenského snažení se řadí i vytvoření jednotného legislativního a terminologického rámce; definice kompetencí jednotlivých státních orgánů na úseku informační bezpečnosti; tvorba standardizovaného rámce; zavedení procesů řízení bezpečnosti ve státní správě; stanovení minimálních požadavků na bezpečnost internetu a elektronické veřejné správy; zvýšení povědomí pracovníků veřejné správy; vymezení postavení CSIRT.SK. Strategie překvapivě vůbec nepracuje v otázkách ochrany lidských práv a svobod s pojmem informačního sebeurčení a obecně je velice vágní.[292] Již zmíněný CSIRT.SK představuje slovenskou jednotku pro řešení počítačových incidentů. Jedná se o specializovaný útvar DataCentra, což je příspěvková organizace Ministerstva financí. CSIRT.SK poskytuje své služby kromě provozovatelů kritické informační infrastruktury i veřejnosti. Je vyloučen pouze z incidentů na úseku utajovaných informací.[293]

Závěr: Česká republika

V průběhu této práce byla představena základní východiska pro diskuzi o existenci informační společnosti a o jejím současném rozvoji. Byly popsány proměny hrozeb, kterým tato společnost denně musí čelit a byl popsán i způsob, jakým se s těmito hrozbami společnost v současnosti vypořádává. Rozsáhlá informatizace veškerých aspektů lidské činnosti a probíhající privatizace klíčových úloh státu jsou fenomény, před kterými není možné se schovat. Zároveň si ale naše civilizace ve 20. století vydobyla určité standardy distributivních práv náležejících jednotlivci a rezignace na ně je v současné době zcela nemožná a nežádoucí. Již proto, jak bylo ostatně prokázáno v textu, musí jakákoli legislativní či jiná úprava kybernetické bezpečnosti reflektovat informační sebeurčení v celé jeho šíři.

V průběhu textu byla také, porovnáváním s úpravami ve vyspělých státech i diskuzí s akademickými prameny, představována připravovaná legislativní úprava kybernetické bezpečnosti v ČR. Byly konstatovány některé aspekty, které jsou inherentní úpravě či snahám vyspělých států na úseku kybernetické bezpečnosti. V rámci výkladu bylo také poukázáno na fakt, že ač některé státy z Pobaltí či z Visegrádské čtyřky přistupují ke kybernetické bezpečnosti velice kreativně a kladou na ni značný důraz, nedaří se dosáhnout standardů, které jsou běžné ve vyspělých státech (snad s výjimkou Estonska, které patří k celosvětové špičce). Strategie se v některých případech zdají být zcela odtržené od toho, co je možné konstatovat jako existující konsensus a někdy dokonce zcela ignorují současný vývoj na poli informačního sebeurčení. Jak již ale bylo zmíněné, maďarské úřady věnující se standardizaci použitých technologií a postupů nebo polská zákonná definice kyberprostoru představují kreativní přístupy a odlišné pohledy na věc. Fakt, že některé legislativní řešení není přítomné v úpravě vyspělých států, nelze v této oblasti považovat za zásadní handicap nebo delegitimizaci případné úpravy.

Česká úprava v podobě současného Návrhu zákona o kybernetické bezpečnosti zdá se být zcela adekvátní tomu, co bylo v této práci konstatováno jako *best practices* při úpravě kybernetické bezpečnosti. Zohledňuje současnou úlohu informačního sebeurčení a zapojuje do kybernetické bezpečnosti soukromý sektor. Jednu z nejdůležitějších otázek, tedy otázku edukace veřejnosti, tomuto budoucímu zákonu nepřísluší řešit. Edukační a propagační činnost by však měla probíhat intenzivně nejenom na úseku kybernetické bezpečnosti, ale i na úseku existence samotného zákona. Z textu této práce je jasné, že separátní úprava není nezbytnou a případná ustanovení by se zřejmě zvládla zakomponovat v rámci novel do již existující legislativy. Takovýto postup by

286 ŚWIĄTKOWSKA 2012 op. cit., s. 42-43.

287 Agencja Bezpieczeństwa Wewnętrznego.

288 Věcný záměr 2012 op. cit., s. 39.

289 *Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* dostupná na http://www.bbn.gov.pl/portal/pl/475/3447/Ustawa_z_30_sierpnia_2011_r_o_zmianie_ustawy_o_stanie_wojennym_oraz_o_kompetencj.html [cit. 16. 3. 2013].

290 Zmíněno ilustrativně tamtéž, odst. 3
Zmíněno i ve Věcný záměr 2012 op. cit., s. 39.

291 *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike* [online]. 2008 [cit. 4. 3. 2013]. 21 s. Dostupné z: http://www.informatizacia.sk/ext_dok--narodna_strategia_pre_ib/6167c.

292 Pro ilustraci: „*Treba vytvoriť dobré právne predpisy, ktoré umožňujú účinne postihovať zistené zločiny smerujúce k poškodzovaniu ľudských práv a slobôd.*" Tento výrok je dále specifikován jako 1) nutnost prosazování demokratických principů při ochraně SR a 2) nutnost legislativně upravit správu osobních údajů tak, aby se s nimi nesměl nikdo seznamovat nad účel jejich správy.
Tamtéž, s. 9-10.

293 *Úvod* [online]. 2013 [cit. 12. 3. 2013]. Dostupné z: http://www.csirt.gov.sk/o-nas-7d6.html.

také vzbudil menší zájem (a zřejmě i odpor) veřejnosti. Fakt, že si legislativec zvolil cestu samostatné legislativní úpravy, také implikuje jistou zodpovědnost při vysvětlování její nutnosti veřejnosti. Kromě této otázky si autor této práce dovolí vyjádřit jistý údiv nad tím, že autoři věcného záměru nepovažovali za nutné zmínit technologickou neutralitu jako jednu z premis budoucího zákona. Technologická neutralita hraje poměrně zásadní roli v německé kybernetické bezpečnosti a měla by být dlouhodobě zdůrazňována nejen pří úpravě kybernetické bezpečnosti, ale při jakýchkoli pokusech o regulaci internetu.

Paragrafové znění zákona, které bylo v tomto roce představeno v podobě Návrhu zákona o kybernetické bezpečnosti, navázalo poměrně kvalitním způsobem na původní Věcný záměr zákona o kybernetické bezpečnosti. Nezatěžuje přehnaně soukromý sektor, což by mělo být hlavním cílem úpravy kybernetické bezpečnosti. Bohužel návrh obsahuje množství odkazů na prováděcí předpisy, což nejspíše nebude na veřejnost či některé povinné osoby působit zcela přijatelně. Také případné sankce za porušení povinností povinnými osobami jsou dle názoru autora příliš nízké a na některé subjekty na trhu by nemuseli působit dostatečně odstrašujícím dojmem.

Vývoj v kyberprostoru je natolik dynamický a turbulentní, že větší úlohu, než samotný zákon, bude zřejmě hrát schopnost uživatelů a bezpečnostních expertů (bez ohledu na to, zdali pocházejí ze sféry veřejné či soukromé) vypořádávat se s novými hrozbami.

Seznam použitých pramenů:

10 Steps to Cyber Security [online]. London: The Information Security Arm of GCHQ, 2012 [cit. 20. 2. 2013]. 22 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73129/12--1121-10-steps-to-cyber-security-advice-sheets.pdf.

10 Steps to Cyber Security: Executive Companion [online]. London: The Information Security Arm of GCHQ, 2012 [cit. 20. 2. 2013]. 20 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf.

2012 Cyber Attacks Statistics [online]. 2013 [cit. 7. 2. 2013]. Dostupné z: http://hackmageddon.com/2012-cyber-attacks--statistics-master-index/.

2012 Data Breach Investigation Report [online]. Verizon, 2012 [cit. 22. 2. 2013]. 76 s. Dostupné z: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations--report-2012_en_xg.pdf.

A Strong Britain in the Age of Uncertainty: The National Security Strategy [online]. London: 2010 [cit. 20. 2. 2013]. 39 s. ISBN 9780101795326. Dostupné z: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.

AFRODITI, Papanastasiou. *Application of International Law in Cyber Warfare Operations* [online]. 2010 [cit. 7. 12. 2012]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1673785.

ALBERTS, David; GARTSKA, John; STEIN, Frederick. *Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd Edition (revised)*. Washington: CCRP Press, 1999. 287 s. ISBN 1-57906-019-6.

ARQUILLA, John; RONFELDT, David (eds.). *Networks and Netwars: Future of Terror, Crime and Militancy.* Santa Monica: RAND Corporation, 2001. 380 s. ISBN 0-8330-3030-2.

As of 1 January 2009, in some cases, submission of the forms TSD and KMD in electronic format shall be mandatory [online]. Estonian Tax and Customs Board [cit. 10. 3. 013]. Dostupné z: http://www.emta.ee/index.php?id=25299.

BAGGILI, Ibrahim (ed.). *Digital Forensics and Cyber Crime.* New York: Springer, 2011 [cit. 15. 9. 2011]. 157 s. ISBN 978-3-642-19513-6.

BAKER, Liana B.; FINKLE, Jim. *Sony PlayStation suffers massive data breach. Reuters.com* [online]. 2011 [cit. 23. 2. 2013]. Dostupné z: http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE-73P6WB20110426.

BANKS, William. *The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber War Draft 9/27/12* [online]. 2012 [cit. 18. 10. 2012]. 30 s. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2160078.

BARLOW, John Perry. *Declaration of Independence of Cyberspace* [online]. Davos: 1996 [cit. 10. 11. 2012]. Dostupné z: https://projects.eff.org/~barlow/Declaration-Final.html.

BASTL, Martin. *Kybernetický terorismus: studia nekonvenčních metod boje v kontextu soudobého válečnictví.* Brno, 2007. 153 s. Disertační práce, Masarykova univerzita, Fakulta sociálních studií.

BENTHAM, Jeremy. *Leviathan* [online]. Project Gutenberg, 2002 [cit. 1. 2. 2013]. Dostupné z: http://www.gutenberg.org/.

Bezpečnostní strategie České republiky [online]. 2011 [cit. 3. 2. 2013]. 21 s. Dostupné z: Www.mzv.cz/file/699914/Bezpecnostni_strategie_CR_2011.pdf.

Bezpečnostní strategie České republiky [online]. Praha: Pro Ministerstvo zahraničních věcí ČR vydalo ediční oddělení Ústavu mezinárodních vztahů, 2003 [cit. 3. 2. 2013]. 28 s. ISBN 8086345459. Dostupné z: Www.army.cz/assets/files/8492/Bezpe_nostn__strategie__R_-prosinec_2003.pdf.

BLAKE, Duncan; IMBURGIA, Joseph S. *„Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as „Weapons."* *Air Force Law Review* [online]. 2010, roč. 66, č. 1, s. 157-204 [cit. 16. 8. 2012]. ISSN 0094-8381. Dostupné z: http://heinonline.org.

BOBEK, Michal; MOLEK, Pavel; ŠIMÍČEK, Vojtěch (eds.). *Komunistické právo v Československu: Kapitoly z dějin bezpráví.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009. 1005 s. ISBN 9788021048447.

BOSWORTH, Seymour; KABAY, M. E. (eds.). *Computer Security Handbook. 4th Edition.* Hoboken: John Wiley & Sons, 2002. ISBN 0471412589.

BRITO, Jerry; WATKINS, Tate. *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. Harvard National Security Journal* [online]. 2011, roč. 3 , č. 1, 39-84 [cit. 16. 8. 2012]. ISSN 2153-1358. Dostupné z: http://heinonline.org.

BRODECKI, Zdisław; NAWROT, Anna Maria. *In Search for Common Sense in Cyberspace. Masaryk University Journal of Law and Technology* [online]. 2008, roč. 2 , č. 2, s.47-61 [cit. 16. 8. 2012]. ISSN 1802-5943. Dostupné z: http://heinonline.org.

BUCHAN, Russell. *Cyber Attacks: Unlawful Use of Force or Prohibited Intervention. Journal of Conflict and Security law* [online]. 2012, roč. 17, č. 2, s. 211-227 [cit. 16. 8. 2012]. ISSN 1467-7962. Dostupné z: http://jcsl.oxfordjournals.org.

BURSTEIN, Aaron J. *Amending the ECPA to Enable a Culture of Cybersecurity Research. Harvard Journal of Law & Technology* [online]. 2008, roč. 22, č. 1, s. 168-222 [cit. 16. 8. 2012]. ISSN 0897-3393. Dostupné z: http://heinonline.org.

CIP Implementation Plan of the National Plan for Information Infrastructure Protection [online]. Federal Ministry of Interior [cit. 4. 3. 2013]. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/UP_KRITIS_en_final.pdf?__blob=publicationFile.

CLARK, Wesley C.; LEVIN, Peter L. *Securing Information Highway. Foreign Affairs* [online]. 2009, roč. 88, č. 6, s. 2-10 [cit. 16. 8. 2012]. ISSN 0015-7120. Dostupné z: http://heinonline.org.

CLEMENTE, Dave. *Defence and Cyber-security: Written Evidence* [online]. 2012 [cit. 25. 2. 2013]. Dostupné z: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm.

COMM, Joel; ROBBINS, Anthony; BURGE, Ken. *Twitter Power.* Hoboken: John Wiley & Sons, 2009. 248 s. ISBN 047058429.

COPPING, Jasper. *Warning over decline in map skills as ramblers rely on sat navs. Telegraph.co.uk* [online]. 2012 [cit. 8. 11. 2012]. Dostupné z: http://www.telegraph.co.uk/earth/countryside/9090729/Warning-over-decline-in-map-skills--as-ramblers-rely-on-sat-navs.html.

COUTS, Andrew. *Senate Kills Cybersecurity Act of 2012. DigitalTrends.com* [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: http://www.digitaltrends.com/web/senate-votes-against--cybersecurity-act-of-2012/.

COVENEY, Peter; HIGHFIELD, Roger. *Mezi chaosem a řádem.* Praha: Mladá fronta, 2003. 428 s. ISBN 8020409890.

Cyber Security Strategy [online]. Tallinn: Ministry of Defence, 2008 [cit. 10. 3. 2013]. 36 s. Dostupné z: http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf.

Cyber Security Strategy for Germany [online]. Berlin: Federal Ministry of the Interior, 2011 [cit. 10. 7. 2012]. 20 s. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

Cyberspace Policy Review [online]. 2009 [cit. 27. 2. 2013]. 76 s. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

DAVIS, Joshua. *Hackers Take Down the Most Wired Country in Europe. Wired.com* [online]. 2007 [cit. 23. 2. 2013]. Dostupné z: http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Défense et sécurité des systèmes d'information: Stratégie de la France [online]. Paris: ANSSI, 2011 [cit. 7. 10. 2012]. 22 s. Dostupné z: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

Demanding the right to digitally protest: Hacktivists petition the White House to legalize DDoS. RT.com [online]. 2013 [cit. 29. 1. 2013]. Dostupné z http://rt.com/usa/news/us-ddos--attacks-legal-736/?utm_medium=referral&utm_source=t.co.

DENNIS, Erin Smith. *A Mosaic Shield: Maynard, The Fourth Amendment, and Privacy Rights in the Digital Age. Cardozo Law Review* [online]. 2011, roč. 33, č. 2, s. 737-771 [cit. 16. 8. 2012]. ISSN 0270-5192. Dostupné z: http://heinonline.org.

Department of Defense Strategy for Operating in Cyberspace [online]. 2011 [cit. 1. 3. 2013]. 19 s. Dostupné z: http://www.defense.gov/news/d20110714cyber.pdf.

DIJK, Jan van. *The Network Society. 3rd edition.* Thousand Oaks: Sage Publications, 2012. 326 s. ISBN 9781446248959.

Domácnosti s připojením k internetu [online]. Český statistický úřad, 2012 [cit. 26. 1. 2013]. Dostupné z: http://notes.czso.cz/csu/redakce.nsf/i/informacni_technologie_pm.

EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse* [online]. Chicago: University of Chicago Legal Forum,1996 [cit. 2. 11. 2012]. 5 s. Dostupné z: http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf.

EGGERS, Matthew. *Enough With the Distractions … It's Time for Consensus-Oriented Cybersecurity Legislation. FreeEnterprise.com* [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: http://www.freeenterprise.com/enough-distractions-it--s-time-consensus-oriented-cybersecurity-legislation.

Estonia Country Report [online]. ENISA, 2011 [cit. 20. 2. 2013]. 30 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Estonia.pdf.

FREEDMAN, James. *Protecting State Secrets as Intellectual Property: A Strategy for Prosecuting Wikileaks. Stanford Journal of International Law.* [online]. 2012, roč. 48, č. 1, s. 185-208 [cit. 17. 5. 2012]. ISSN 0731-5082. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042692.

GARDHAM, Duncan. *Britain Prepares for Cyber War. Telegraph.co.uk* [online]. 2011 [cit. 25. 2. 2013]. Dostupné z: http://www.telegraph.co.uk/news/uknews/defence/8915871/Britain-prepares-for-cyber-war.html.

GEER, Daniel E. *Cybersecurity and National Policy. Harvard National Security Journal* [online]. 2010, roč. 1, č. 1, s. 203-215 [cit. 12. 9. 2012]. ISSN 2153-1358. Dostupné z: http://www.harvardnsj.com/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf.

GEERS, Kenneth. *Strategic Cyber Security* [online]. Tallinn: CCD COE Publication, 2011 [cit. 15. 9. 2012]. 168 s. ISBN 978-9949-9040-7-5. Dostupné z: http://www.ccdcoe.org/278.html.

Germany Country Report [online]. ENISA, 2011 [cit. 20. 2. 2013]. 47 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf.

GJELTEN, Tom. *Volunteer Cyber Army Emerges in Estonia. NPR.org* [online]. 2011 [cit. 10. 3. 2013]. Dostupné z: http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer--cyber-army-defends-nation.

GOODIN, Dan. *Why the Red October Malware is the Swiss Army Knife of Espionage. ArsTechnica.com* [online]. 2013 [cit. 20. 2. 2013]. Dostupné z: http://arstechnica.com/security/2013/01/why-red-october-malware-is-the--swiss-army-knife-of-espionage/.

GRAHAM, James; HOWARD, Richard; OLSON, Ryan (eds.). *Cyber Security Essentials.* Boca Raton: CRC Press, 2011. 325 s. ISBN 978-1-4398-5123-4.

GROSSMANN, D. *On Killing: The Psychological Cost of Learning to Kill in War and Society.* Boston: Little Brown, 1995. 367 s. ISBN 0316330000.

HABER, Eldar. *The French Revolution 2.0: Copyright and the Three Strikes Policy. Harvard Journal of Sports and Entertainment Law* [online]. 2011, roč. 2, č. 2, s. 298-339 [cit. 20.2.2012]. ISSN 2153-1323. Dostupné z: http://heinonline.org.

Hackeři zveřejnili osobní data 57 tisíc zákazníků CS Link a Skylink. Novinky.cz [online]. 2012 [cit. 28. 1. 2013]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/287836-hackeri-zverejnili-osobni-data-57-tisic-zakazniku-cs-link-a-skylink.html.

HARTZOG, Paul B. *Panarchy: Governance in the Network Age.* [online]. Salt Lake City, 2005 [cit. 10. 11. 2012]. Diplomová práce. University of Utah. Dostupné z: http://www.academia.edu/210378/Panarchy_Governance_in_the_Network_Age.

HAVRÁNEK, Bohuslav (red.). *Slovník spisovné češtiny* [online]. Ústav pro jazyk český ČSAV, 2011 [cit. 10. 2. 2013]. Dostupné z: http://ssjc.ujc.cas.cz/.

HERBERT, Ian. *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence. Berkeley Journal of Criminal Law* [online]. 2011, roč. 16, č. 2, s. 442-505 [cit. 10. 3. 2013]. Dostupné z: http://www.bjcl.org/archives/16_2/herbert_formatted.pdf.

HOLLÄNDER, Pavel. *Základy všeobecné státovědy. 3.vydání.* Plzeň: Aleš Čeněk, 2012. 429 s. ISBN 9788073803957.

HOLLIS, David. *Cyberwar Case Study: Georgia 2008. Small Wars Journal* [online]. 2011, roč. 7, č. 1, s. 1-10 [cit. 1. 10. 2012]. ISSN 0737-1217. Dostupné z: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Hungary Country Report [online]. ENISA, 2011 [cit. 16. 10. 2013]. 30 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Hungary.pdf.

Hungary's National Security Strategy [online]. Ministry of Foreign Affairs, 2012 [cit. 22. 2. 2013]. 23 s. Dostupné z: http://www.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf.

Hungary's National Cyber Security Strategy of Hungary [online]. 2013. [cit. 16. 10. 2013]. 7 s. Dostupné z: http://nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx.

CHANG, Ha-Joon. *23 Things They Don't Tell You About Capitalism.* London: Allen Lane, 2011. 286 s. ISBN 9781846143281.

International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World [online]. Washington: The White House, 2011 [cit. 3. 3. 2013]. 25 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Internet Voting in Estonia [online]. Vabariigi Valimiskomisjon [cit. 10. 3. 2013]. Dostupné z: http://www.vvk.ee/voting-methods-in-estonia/engindex/.

ISANGA, Joseph M. *Counter-Terrorism and Human Rights: The Emergence of a Rule of Customary International Law from United Nations Resolutions. Denver Journal of International Law and Policy* [online]. 2009, roč. 37, č. 2, s. 223-255 [cit. 29. 6. 2012]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2093414.

ITU National Cybersecurity Strategy Guide [online]. 2011 [cit. 1. 10. 2012]. 119 s. Dostupné z: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

JIRÁSEK, Petr; KNÝ, Milan (eds.). *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR & Česká pobočka AFCEA, 2012 [cit. 29. 1. 2013]. ISBN 978-80-7251-378-9. Dostupné z: www.cybersecurity.cz/data/slovnik_v150.pdf.

Kasperski Lab Identifies Operation „Red October", an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide [online]. 2013 [cit. 23. 2. 2013]. Dostupné z: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

KAUFFMAN, Stuart A. *At home in the universe: the search for laws of self-organization and complexity.* New York: Oxford Unviersity Press, 1995. 321 s. ISBN 0195111303.

KETTEMANN, Matthias. *UN Human Rights Council Confirms that Human Rights Apply to the Internet. EJIL: Talk!* [online]. 2012 [cit. 25. 7. 2012]. Dostupné z: http://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/.

Key 2006-2013 ICT data [online]. International Telecommunication Union, 2013 [cit. 16. 10. 2013]. Dostupné z: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

KLIMBURG, Alexander. *The Whole of Nation in Cyberpower. Georgetown Journal of International Affairs* [online]. 2011, zvláštní vydání, s. 171-179 [cit. 16. 8. 2012]. ISSN 1526-0054. Dostupné z: http://heinonline.org.

KLIMEK, Libor. *Combating Attacks Against Information Systems: EU Legislation and its Development. Masaryk University Journal of Law and Technology*. 2012, roč. 6, č 1, s. 87-100. ISSN 1802-5943.

KMEC, Jiří. Ústavní soudci, mluvíte spolu? Jiné Právo [online]. 2010 [cit. 24. 1. 2013]. Dostupné z: http://jinepravo.blogspot.cz/2010/05/ustavni-soudci-mluvite-spolu.html.

KNAP, Karel et al.. *Ochrana osobnosti podle občanského práva. 4. podstatně přepracované a doplněné vydání.* Praha: LINDE, 2004. 435 s. ISBN 8072014846.

KOZÁK, Karel. *Revoluce ve vojenských záležitostech.* Vojenské rozhledy. 2001, roč. 10, č. 4, s. 67-84. ISSN 1210-3292.

KUHLMANN, Stephanie A. *Do Not Track Me Online: The Logistical Struggles over the right „to be let alone" online. DePaul Journal of Art, Technology & Intellectual Property Law* [online]. 2011, roč. 22, č. 1, s. 229-286 [cit. 16. 8. 2012]. Dostupné z: http://heinonline.org.

KÜHN, Zdeněk. *Jak zlepšit české právní informační systémy? Jiné Právo* [online]. 2008 [cit. 7. 9. 2012]. Dostupné z: http://jinepravo.blogspot.cz/2008/02/jak-zlepit-esk-prvn-informan-systmy.html.

LA RUE, Frank. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* [online]. UN General Assembly, 2011 [cit. 27. 1. 2013]. Dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Latvia Country Report [online]. ENISA, 2011 [cit. 20. 2. 2013]. 25 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Latvia.pdf/at_download/file.

LENNON, Mika. *Threat from Cyber Attacks Nearing Statistical Certainty. SecurityWeek.com* [online]. 2011 [cit. 23. 2. 2013]. Dostupné z: http://www.securityweek.com/threat--cyber-attacks-nearing-statistical-certainty.

LESSIG, Lawrence. *Code: version 2.0* [online]. New York: Basic Books, 2006 [cit. 9. 12. 2012]. 410 s. ISBN 0465039146. Dostupné z: http://codev2.cc/download+remix/Lessig-Codev2.pdf.

LÉVY, Pierre. *Kyberkultura: zpráva pro Radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace"*. Praha: Karolinum, 2000. 229 s. ISBN 8024601095.

Lithuania Country Report [online]. ENISA, 2011 [cit. 20. 2. 2013]. 24 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Lithuania.pdf.

MAIER, Bernhard. *How Has the Law Attempted to Tackle the Borderless Nature of the Internet. International Journal of Law and Information Technology* [online]. 2010, roč. 18, č. 2, s. 142-175 [cit. 16. 8. 2012]. ISSN 1464-3693. Dostupné z: http://ijlit.oxfordjournals.org/.

MARKOFF, John. *Old Tricks Threatens the Newest Weapons. NYTimes.com* [online]. 2009 [cit. 20. 2. 2013]. Dostupné z: http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all&.

MCLAURIN, Joshua. *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks. Yale Law & Policy Review* [online]. 2011, roč. 30, č. 1, s. 211-254 [16. 8. 2012]. ISSN 0740-8048. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1966269.

MCLUHAN, Marshall. *Understanding media: the extensions of man*. Cambridge: MIT Press, 1995. 365 s. ISBN 0262631598.

MICHAELS, Jon D. *Private Military Firms, American Precedent, and the Arab Spring. Stanford Journal of International Law* [online]. 2012, roč. 48, č. 2, s. 277-288 [cit. 19. 10. 2013]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2160550.

NAKASHIMA, Ellen. *Obama signs secret directive to help thwart cyberattacks. WashingtonPost.com* [online]. 2012 [cit. 9. 3. 2013]. Dostupné z: http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense.

Národná stratégia pre informačnú bezpečnosť v Slovenskej republike [online]. 2008 [cit. 4. 3. 2013]. 21 s. Dostupné z: http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c.

National Security Strategy [online]. Washington: The White House, 2010 [cit. 27. 2. 2013]. 52 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

National Strategy for Trusted Identities in Cyberspace [online]. Washington: The White House, 2011 [cit. 2. 3. 2013]. 45 s. Dostupné z: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Nejde nám o peníze, ale o názor, tvrdí hackeři. Ekonom. 2013, č. 4, s. 8-9. ISSN 1213-7693.

O'CONNELL, Marry Ellen. *Cyber Security without Cyber War. Journal of Conflict and Security Law* [online]. 2012, roč. 17, č. 2, s. 187-209 [cit. 16. 8. 2012]. ISSN 1467-7962. Dostupné z: http://jcsl.oxfordjournals.org.

OECD Ministerial Background Report DSTI/ICCP/Reg(2007)/20/FINAL Development of Policies for Protection of Critical Information Infrastructure [online]. 2007 [cit. 9. 12. 2012]. 101 s. Dostupné z: www.oecd.org/dataoecd/25/10/40761118.pdf.

PAGET, François. *White Paper on Hacktivism* [online]. 2012 [cit. 20. 2. 2013]. 34 s. Dostupné z: http://www.mcafee.com/hk/resources/white-papers/wp-hacktivism.pdf.

PCs In-Use Worldwide reaches over 1.6BUnits in 2011. USA has nearly 311M PCs In-Use [online]. ETForecasts, 2012 [cit. 8. 11. 2012]. Dostupné z: http://www.etforecasts.com/pr/pr020112.htm.

PITÁKOVÁ, Jaroslava. *Kybernetická bezpečnosť: teoretická analýza a jej praktické uplatnenie vo vybraných štátoch.* Brno, 2012. 118 s. Diplomová práce, Masarykova univerzita, Fakulta sociálních studií.

POKORNÝ, Milan (red.). *Nejvyšší soud o občanském soudním řízení v některých věcech pracovněprávních, občanskoprávních a rodinněprávních: sborník stanovisek, závěrů, rozborů a zhodnocení soudní praxe, zpráv o rozhodování soudů a soudních rozhodnutí Nejvyššího soudu. 1964-1969.* Praha: SEVT, 1980. 439 s.

POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3.

POOLE, John Bernard et al. *Education for an Information Age: Teaching in the Computerized Classroom. 7th Edition* [online]. 2009 [cit. 8. 11. 2012]. Dostupné z: http://www.pitt.edu/~poole/InfoAge7frame.html

PORCHE, Isaac R. III; SOLLINGER, Jerry M.; MCKAY, Shawn. *A Cyberworm that Knows no Boundaries.* [online]. Santa Monica: RAND Corporation, 2011 [cit. 12. 9. 2012]. 55 s. Dostupné z: http://www.rand.org/pubs/occasional_papers/OP342.html.

Progress Against the Objectives of the National Cyber Security Strategy – December 2012 [online]. 2012 [cit. 20. 2. 2013]. 6 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf.

RAHMAN, Rizal. *The legal measure against Denial of Service (DoS) attacks adopted by the United Kingdom legislature: should Malaysia follow suit? International Journal of Law and Information Technology* [online]. 2012, roč. 20, č. 2, s. 85-101 [cit. 16. 8. 2012]. ISSN 1464-3693. Dostupné z: http://ijlit.oxfordjournals.org/.

REITMAN, Rainey. *New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities* [online]. 2012 [cit. 4. 3. 2013]. Dostupné z: https://www.eff.org/deeplinks/2012/07/new--cybersecurity-proposal-patches-serious-privacy-vulnerabilities.

RICHMOND, Riva. *Malware Hits Computerized Industrial Equipment. NYTimes.com* [online]. 2010 [cit. 22. 2. 2013]. Dostupné z: http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/.

RYŠKA, Michal. *O mantinelech soukromí a informačním sebeurčení (a taky o chování na veřejnosti, Zeleném Raoulovi a upovídané pacientce). Jiné Právo* [online]. 2010 [cit. 12. 12. 2012]. Dostupné z: http://jinepravo.blogspot.cz/2010/08/michal-ryska-o-mantinelech-soukromi.html.

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 [online]. 2010 [cit. 1. 3. 2013]. 33 s. Dostupné z: http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf.

SALOMON, Jean-Jacques. *Technologický úděl.* Praha: Filosofia, 1997. 287 s. ISBN 8070070978.

SAPETKAITĖ, Vaiva. *Kibernetinis (ne)saugumas: Baltijos šalių situacija.* Geopolitika.lt [online]. 2012 [cit. 20. 2. 2013]. Dostupné z: http://www.geopolitika.lt/?artc=5504.

Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review [online]. London: 2010 [cit. 20. 2. 2013]. 75 s. ISBN 9780101794824. Dostupné z: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf.

SHACKELFORD, Scott J. *Estonia Two-and-a-Half-Years Later: A Progress Report on Combating Cyber Attacks* [online]. 2009 [cit. 16. 8. 2012]. 12 s. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849.

SHACKELFORD, Scott J. *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal of International Law* [online]. 2009, roč. 27, č. 1, s. 192-251 [cit. 16. 8. 2012]. ISSN 1085-5718. Dostupné z: http://heinonline.org.

SHACKELFORD, Scott J.; ANDRES, Richard B. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Georgetown Journal of International Law* [online]. 2011, roč. 42, č. 4, s. 971-1016 [cit. 16. 8. 2012]. ISSN 1550-5200. Dostupné z: http://heinonline.org.

SMEJKAL, Vladimír a kol. *Právo informačních a komunikačních systémů. 2. aktualizované a rozšířené vydání.* Praha: C. H. Beck, 2004. 770 s. ISBN 8071797650.

SOLCE, Natasha. *The Battlefield of Cyberspace: The Inevitable New Military branch – The Cyber Force. Albany Law Journal of Law & Technology* [online]. 2008, roč. 18, č. 1, s. 293-324 [cit. 16. 8. 2012]. ISSN 1059-4280. Dostupné z: http://heinonline.org.

SOMAIYA, Ravi. *Hackers Shut Down Government Sites. NYTimes.com* [online]. 2011 [cit. 22. 2. 2013]. Dostupné z: http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html?_r=2&.

Sony admits personal data was not encrypted. Bit-tech.net [online]. 2011 [cit. 29. 1. 2013]. Dostupné z: http://www.bit-tech.net/news/gaming/2011/04/28/sony-admits-personal-data-was-not-encrypted/1.

Student ‚Twitters' his way out of Egyptian jail. CNN.com [online]. 2008 [cit. 4. 11. 2012]. Dostupné z: http://articles.cnn.com/2008-04-25/tech/twitter.buck_1_cell-phone--blog-anti-government-protest?_s=PM:TECH.

SULER, John. *The Online Disinhibition Effect* [online]. 2004 [cit. 12. 1. 2013]. Dostupné z: http://users.rider.edu/~suler/psycyber/disinhibit.html.

SULLIVAN, Claire. *Digital Identity and Mistake. International Journal of Law and Information Technology* [online]. 2012, roč. 20, č. 3, s. 223-241 [cit. 16. 8. 2012]. ISSN 1464-3693. Dostupné z: http://ijlit.oxfordjournals.org/.

ŚWIĄTKOWSKA, Joanna (ed.). *V4 cooperation in ensuring cyber security – analysis and recommendations.* Kraków: The Kosciuszko Institute, 2012. 85 s. ISBN 9788393109364.

ŠAVELKA, Jaromír. *Jak zlepšit zpřístupňování judikatury? Jiné Právo* [online]. 2012 [cit. 7. 9. 2012]. Dostupné z: http://jinepravo.blogspot.cz/2012/04/jaromir-savelka-jak-zlepsit.html.

ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. 212 s. ISBN 9788021054493.

The IT Security Situation in Germany in 2011 [online]. Bonn: Federal Office for Information Security, 2011 [cit. 4. 3. 2013]. 48 s. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2011_pdf.pdf?__blob=publicationFile.

The National Strategy to Secure Cyberspace [online]. Washington: The White House, 2003 [cit. 12. 9. 2012]. 60 s. Dostupné z: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 [online]. Vilnius, 2011 [20. 2. 2013]. 17 s. Dostupné z: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf.

The UK Cyber Security Strategy Report on Progress December 2012 – Forward Plans [online]. 2012 [cit. 20. 2. 2013]. 9 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83757/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf.

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world [online]. London: 2011 [cit. 20. 2. 2013]. 43 s. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. *International Cyber Incidents: Legal Considerations* [online]. Tallinn: CCD COE Publications, 2010 [cit. 15. 5. 2012]. 130 s. ISBN 978-9949-9040-0-6. Dostupné z: http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

TIKK, Eneken. *Comprehensive Legal Approach to Cyber Security* [online]. Tallinn, 2011 [cit. 3. 9. 2012]. 170 s. Disertační práce, University of Tartu, Právnická fakulta. ISBN 978-9949-19-763-7. Dostupné z: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1.

TIKK, Eneken. *Ten Rules for Cyber Security. Survival: Global Politics and Strategy* [online]. 2011, roč. 53, č. 3, s. 119-132 [cit. 1. 8. 2012]. ISSN 1468-2699. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2011.571016.

TSAGOURIAS, Nicholas. *Cyber attacks, self-defense and the problem of attribution. Journal of Conflict and Security Law* [online]. 2012, roč. 17, č. 2, s. 229-244 [cit. 16. 8. 2012]. ISSN 1467-7962. Dostupné z: http://jcsl.oxfordjournals.org.

United Kingdom Country Report [online]. ENISA, 2011 [cit. 20. 2. 2013]. 52 s. Dostupné z: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/UK.pdf.

Úvod [online]. 2013 [cit. 12. 3. 2013]. Dostupné z: http://www.csirt.gov.sk/o-nas-7d6.html.

Vybavenost domácností osobních počítačem a internetem podle typu domácnosti, velikosti obce příjmové skupiny krajů [online]. Český statistický úřad [cit. 26. 1. 2013]. Dostupné z: http://vdb.czso.cz/vdbvo/tabparam.jsp?childsel0=1&cislota-b=ICT0070PU_KR&kapitola_id=420&voa=tabulka&go_zobraz=1&childsel0=1

WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, 2005. 159 s. ISBN 8086898210.

War in the fifth domain. Economist.com [online]. 2010 [cit. 1. 3. 2013]. Dostupné z: http://www.economist.com/node/16478792.

WARREN, Samuel; BRANDEIS, Louis D. *The Right to Privacy. Harvard Law Review* [online]. 1890, roč. 6, č. 5 [cit. 12. 12. 2012]. ISSN 0017-811X. Dostupné z: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

WEBSTER, Frank. *Theories of the Information Society. Third edition.* London: Routledge, 2006. 317 s. ISBN 0-415-40633-1.

WEISS, Gus W. *The Farewell Dossier: Duping the Soviets* [online]. 2007 [cit. 20. 2. 2013]. Dostupné z: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.

WIENER, Norbert. *Kybernetika a společnost.* Praha: Československá akademie věd, 1963. 216 s.

WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s.

WORTZEL, Larry M. *China's approach to Cyber Operations: Implications for the United States* [online]. 2010 [cit. 22. 2. 2013]. 11. sDostupné z: http://origin.www.uscc.gov/china-%E2%80%99s-approach-cyber-operations-implications-united-states.

ZEMAN, Petr (ed.). Česká bezpečnostní terminologie: výklad základních pojmů [online]. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002 [cit. 16. 10. 2013]. 186 s. ISBN 8021030372. Dostupné z: www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.

ZLATUŠKA, Jiří. *Informační společnost. Zpravodaj ÚVT MU* [online]. 1998, roč. 8, č. 4, s. 1-6 [cit. 9. 11. 2012]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/articles/122.html.