MASARYKOVA UNIVERZITA
PRÁVNICKÁ FAKULTA

Radim Polčák, Jakub Harašta, Václav Stupka

PRÁVNÍ PROBLÉMY KYBERNETICKÉ BEZPEČNOSTI

ACTA UNIVERSITATIS BRUNENSIS

IURIDICA
Editio Scientia vol. 576

SPISY PRÁVNICKÉ FAKULTY
MASARYKOVY UNIVERZITY

řada teoretická, Edice Scientia
svazek č. 576

PRÁVNÍ PROBLÉMY KYBERNETICKÉ BEZPEČNOSTI

Radim Polčák, Jakub Harašta, Václav Stupka

Masarykova univerzita
Brno 2016

Vzor citace
POLČÁK, Radim ; HARAŠTA, Jakub ; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016. 215 s. Spisy Právnické fakulty MU, řada teoretická, edice Scientia, sv. č. 576. ISBN 978-80-210-8426-1.

CIP - Katalogizace v knize

POLČÁK, Radim
Právní problémy kybernetické bezpečnosti / Radim Polčák, Jakub Harašta, Václav Stupka. --1. vydání. -- Brno: Masarykova univerzita, 2016. 215 stran. – Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia, svazek č. 576. ISBN 978-80-210-8426-1 (brož.)

351.78:004.7* 004.056* 004.996(1)* 355.01:004.7* 343.3/.7:004* (048.8:082)*
- kybernetická bezpečnost
- informační bezpečnost
- kyberprostor
- kybernetická válka
- počítačová kriminalita
- kolektivní monografie

351 – Úkoly veřejné správy, správní opatření, legislativa [15]

Tato publikace vznikla na Masarykově univerzitě v rámci projektu „Právní problémy kybernetické bezpečnosti“ č. MUNI/A/1192/2015 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2016.

Autoři:

doc. JUDr. Radim Polčák, Ph.D.	kap. 1, 2, 3, 4, 5
Mgr. Václav Stupka	kap. 6, 7, 8, 9
JUDr. Jakub Harašta	kap. 10, 11, 12

Recenzent: doc. JUDr. Ladislav Pokorný, Ph.D.

ISBN 978-80-210-8426-1

OBSAH

1 POJEM KYBERNETICKÉ BEZPEČNOSTI V ČESKÉM PRÁVU 9
1.1 Metodologie práva kybernetické bezpečnosti 9
1.2 Základy legislativního řešení kybernetické bezpečnosti 12
1.3 Principy české a evropské právní úpravy kybernetické bezpečnosti 17

2 INSTITUTY ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI 27
2.1 Bezpečnostní opatření 28
2.2 Protiopatření 30
2.3 Odpovědnost za nedbalost a prevenční povinnosti 33
2.4 Disciplinární odpovědnost a disciplinární povinnosti 36

3 INDIVIDUÁLNÍ ODPOVĚDNOST ZA KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT 41
3.1 Kybernetická bezpečnost jako agenda výkonné moci 41
3.2 Individuální odpovědnost a ochrana prostředí 42
3.3 Postih nezodpovědného uživatele 45
3.4 Postih příliš aktivního operátora 48
3.5 Interní instrukce jako bezpečnostní opatření 51
3.6 Nevhodný obsah interních bezpečnostních instrukcí 52
3.7 Zákonná konformita interní instrukce 56
3.8 Srozumitelnost interní instrukce a bezpečnost z podstaty 58
3.9 Interní instrukce a problém soukromí na pracovišti 60

4 PERSPEKTIVY DALŠÍHO VÝVOJE ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI 65
4.1 Zákonná typologie uživatelů vybraných systémů a sítí 66
4.2 Omezená odpovědnost běžných uživatelů 68
4.3 Specifická úprava outsourcingu 70
4.4 Další vývojové perspektivy práva kybernetické bezpečnosti 72

5 PERSPEKTIVY DALŠÍHO POLITICKÉHO A ORGANIZAČNÍHO VÝVOJE AGENDY KYBERNETICKÉ BEZPEČNOSTI V ČR 75
5.1 Certifikace a compliance check 75
5.2 Aktivní obrana – best practices 82
5.3 Kybernetická bezpečnost jako agenda podpory investic 84
5.4 Kybernetická bezpečnost jako agenda rozvojové pomoci 86

6 MECHANISMY ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI 89
6.1 Spolupráce na národní úrovni 90
6.2 Spolupráce na mezinárodní úrovni 93

7 POVINNOSTI SPRÁVCŮ INFRASTRUKTUR 95
7.1 Skupiny povinných osob dle ZoKB 95
7.2 Povinnosti povinných osob dle ZoKB 99
7.3 Nové povinné osoby a jejich povinnosti v ZoKB podle směrnice NIS 102
7.4 Povinnosti vyplývající s ostatních právních předpisů 106

8 SDÍLENÍ INFORMACÍ V KYBERNETICKÉ BEZPEČNOSTI 109
8.1 Sběr informací pomocí analýzy datového provozu 109
8.2 Dobrovolné sdílení informací v kybernetické bezpečnosti 117
8.3 Exkurs – srovnání přístupu v ZoKB s úpravou sdílení informaci v USA 120

9 SPOLUPRÁCE BEZPEČNOSTNÍCH SLOŽEK 125
9.1 Orgány činné v trestním řízení 125
9.2 Zpravodajské služby 136
9.3 Kybernetická obrana 138

10 VYMEZENÍ ZÁJMU STÁTU V KYBERPROSTORU 141
10.1 Kybernetická a informační suverenita 141
10.2 Česká republika: hodnotové zakotvení 151

11 KYBERNETICKÁ VÁLKA A POUŽITÍ SÍLY 161
11.1 Clausewitz a „kybernetická válka“ 161
11.2 Kybernetická operace jako použití síly 168

12 TECHNOLOGICKÁ VÝZVA HUMANITÁRNÍMU PRÁVU .. 179
12.1 Martensova klauzule 179
12.2 Rozlišování při použití kybernetických prostředků 187

Summary 201
Literatura a další použité zdroje 203

1 POJEM KYBERNETICKÉ BEZPEČNOSTI V ČESKÉM PRÁVU[1]

1.1 Metodologie práva kybernetické bezpečnosti

Obecně lze v právním instrumentariu nalézt tři typy právních metod, a to metody pozitivistické, naturalistické a realistické (či pragmatické). Pozitivistické metody vyznačují se pojmovým oddělením pravidel od faktických dat[2]. Znamená to mimo jiné, že pravidlo nemůže svým obsahem vycházet z informace o skutečnosti (z výroku), ale je vždy vytvořeno jako originální informace o povinnostech. Fakticita se zde v obsahu pravidel nijak neprojevuje a s fakty pracujeme pouze jako s faktory naplnění subsumpčních podmínek[3]. Jinak řečeno je tedy v tomto metodologickém pojetí právo systémem originálně tvořených instrukcí a fakta jsou pro právo důležitá pouze co do rozhodování v otázce, zda právo pro konkrétní situace formuluje nějaké konkrétní imperativy (tj. v otázce, zda jsou ad hoc naplněny znaky hypotéz příslušných právních norem).

Obecně se oddělení faktických a povinnostních dat u právního pozitivismu projevuje absencí vztahu mezi právem a morálkou[4]. Morálka jako faktická kategorie totiž nemůže v pozitivistickém pojetí práva ovlivňovat obsah

1 Tato kapitola a kap. 2, 4 a 5 jsou založeny na výzkumu, jehož výsledky byly částečně publikovány v článku Polčák, R. Kybernetická bezpečnost jako aktuální fenomén českého práva, Revue pro právo a technologie, roč. 6, číslo 11, str. 95.

2 Toto oddělení je založeno na Humově základní filozofické distinkci mezi bytím (is) a mětím (ought) – viz Hume, D. A Treatise on Human Nature. Project Gutenberg, 2003, dostupný on-line na adrese www.gutenberg.org/etext/4705.

3 Kelsen označuje toto pojetí práva za „ryzí," tj. oproštěné od všeho, co do něj nepatří – viz Kelsen, H. Pure Theory of Law, přel. Knight, M. Berkeley: University of California Press, 1978, str. 1.

4 K tomu srov. např. Alexy, R. The Argument from Injustice, přel. Paulson, S., Litschewski Paulson, B. Oxford: Oxford University Press, 2002, str. 85 a násl.

právních pravidel[5]. To samozřejmě neznamená, že právní pravidla musí být nutně amorální – jejich konstrukci ani aplikaci však morálka v tomto pojetí přímo neovlivňuje.

V oboru práva informačních a komunikačních technologií se základní motiv pozitivistické metodologie projevuje neexistencí přímého vztahu mezi faktickou situací určité technologie (tj. jejími parametry, fungováním apod.) a obsahem právních pravidel regulujících její užití. Důsledná aplikace pozitivistické metodologie v tomto směru může vést k takovým důsledkům, kdy je formulován právně perfektní (bezvadný) právní předpis nebo soudní rozhodnutí, jejichž praktická aplikace je z nějakého praktického důvodu vyloučena – k tomu může dojít tehdy, jsou-li např. stanoveny nereálné požadavky na nějakou technologii, právo požaduje řešení, které nelze organizačně zvládnout nebo je vyžadováno splnění takové povinnosti, která je z ekonomického hlediska absurdní. Z právě uvedeného plyne, že užití této metody k řešení problému kybernetické bezpečnosti není vhodné[6].

Druhou možností je naturalistická právní metodologie[7] postavená ve vztahu k pozitivismu na zcela opačné tezi spojení faktických a povinnostních dat. Obecnou implikací této teze je možnost přímého dovození právních pravidel z morálky a jí odpovídající předpoklad, že objektivní právo je jen konstatováním existence přirozených pravidel (de facto přírodních zákonů) a že právotvorba není ve skutečnosti o originárním vytváření právních pravidel ale pouze o jejich nalézání.

Aplikace naturalistické metodologie v právu informačních a komunikačních technologií vede k závěru formulovanému předním americkým konstitucionalistou Lawrencem Lessigem, že totiž „kód je zákonem kyberprostoru.[8]“ Znamená to, že právo pro informační síť je resp. má být pouze

5 Kritiku nedostatku tohoto přístupu spočívajícího obecně v pojmové nemožnosti hodnotové reflexe obsahu platného práva je možno najít např. v díle Vladimíra Čemáka – viz Baroš, J. (ed.) Vladimír Čermák – člověk, filozof, soudce. Brno: Masarykova univerzita, 2009, str. 248.

6 Nepomáhá v tomto směru ani výjimečná zásada impossibilium nulla obligatio – její aplikace je totiž podmíněna aletickou nemožností. V technologicky exponovaných situacích však je nutno z pohledu práva nezřídka šlápnout i na kluzký svah organizační resp. obchodní nemožnosti. To je pro právní pozitivismus neakceptovatelné, neboť může následná normativní eroze vést až k důsledkům shrnutelným slovy klasika do postulátu „když nemůžu, tak nemusím.“

7 Obecně k pojmu viz Finnis, J. Natural Law. New York: New York University Press, 1991.

8 Viz Lessig, L. Code V. 2. New York: Basic Books, 2006.

dovozováno z technických pravidel definujících možnosti chování uživatele. Lessigem popsaný stav již v řadě ohledů reálně funguje. Především v případech, kdy brání uplatnění práva některý z právních nebo přirozených limitů (tj. např. otázka jurisdikce, absence věcné působnosti, vysoké náklady na výkon práva apod.), je kód skutečně dominantním normativním faktorem ovlivňujícím, často výlučně, chování uživatelů.

Z právě popsaného důvodu nelze však s iusnaturalistickou metodologií pracovat pro potřeby řešení problému kybernetické bezpečnosti. Přijetí tohoto přístupu by totiž v prostředí informačních sítí znamenalo popření základní premisy, na níž zde v současnosti stojí legitimita práva, tj. že právo je legitimováno veřejným zájmem. Iusnaturalistické pojetí totiž přisuzuje možnost definovat obsah právních pravidel subjektům majícím pod kontrolou technické parametry příslušných součástí informační sítě, z nichž většinou jde o soukromoprávní korporace.

Nikoli jen vylučovací metodou jeví se jako nejvhodnější k řešení problému kybernetické bezpečnosti metoda realistická[9]. Je postavena na podobném předpokladu jako právní pozitivismus, tj. že obsah právních pravidel je originárně vytvářen a je zajišťován autoritou státu, avšak netrvá na důsledném pojmovém oddělení právních pravidel od faktických dat. Zohlednění faktičnosti, ať technické, ekonomické nebo organizační, má formu omezení legislativních a aplikačních výstupů o ty, které jsou prakticky (pragmaticky) neproveditelné[10]. Pragmatický zákon tedy počítá jen s takovými povinnostmi, které je reálně možno splnit bez větší zátěže pro povinné subjekty a soudní rozhodnutí je založeno na předpokladu reálné (nikoli ideální) společenské, technické a ekonomické situace[11].

Zřejmá nevýhoda realistické metodologie spočívá především v riziku relativizace právních hodnot, neboť tam, kde se jejich důsledná aplikace odchyluje od toho, co považujeme za součást technické, společenské nebo

9 Používá se též výrazu pragmatismus – k tomu viz např. James, W. Pragmatism. Rockville: ARC Manor, 2008 nebo Tamanaha, B. Beyond the Formalist – Realist Divide. Princeton: Princeton University Press, 2010, str. 67 a násl.

10 K tomu viz např. Rorty, R. The Banality of Pragmatism and the Poetry of Justice. Southern California Law Review. 1990, roč. 63, str. 1811 a násl.

11 Srov. Sharp, W.G. Sr. The Past, Present and Future of Cybersecurity, Journal of National Security Law and Policy, roč. 4, číslo 13, str. 19 a násl.

ekonomické reality, prostě od nich ustoupíme. To může vést k Dworkinem kritizovanému postupnému úbytku ideálů[12] a nebezpečí tvorby situací, kdy právo jen kopíruje požadavky ekonomické, technické nebo obecně společenské reality resp. toho, co je za realitu aktuálně považováno politickou mocí. Na druhou stranu však realistická metodologie poskytuje jako jediná z uvedených alternativ prakticky použitelná řešení pro situace vyznačující se značnou mírou technické, ekonomické či společenské složitosti a právě takovou situací je současný stav informační společnosti[13]. Udržení úrovně hodnot a principů, jakož i idealistického charakteru právních pravidel je v tomto případě řešeno nikoli metodologicky ale institucionálně prostřednictvím legitimity orgánů veřejné moci zajišťujících tvorbu příslušných právních pravidel a jejich následnou implementaci[14]

1.2 Základy legislativního řešení kybernetické bezpečnosti

Legislativní řešení kybernetické bezpečnosti nemá v platném právu žádnou prakticky srovnatelnou paralelu. Lze sice pro partikulární otázky používat nejrůznější analogie s bezpečnostními řešeními v oborech s dominantní technologickou komponentou (typicky např. v oborech stavebnictví, protipožární ochrany, dopravy, apod.), právní fenomén kybernetické bezpečnosti se však jako takový ničemu ve své podstatě nepodobá[15].

Prvním důvodem originality kybernetické bezpečnosti je skutečnost, že hodnocení bezpečnostních aktiv má až na výjimky obvykle akcesorickou povahu. Systémy a sítě, jejichž zabezpečení je předmětem právní úpravy,

12 Viz Dworkin, R. Justice in Robes. London: Belknap Press, 2006, str. 38.

13 Viz Polčák, R. Internet a proměny práva, Praha: AUDITORIUM, 2012, str. 85.

14 K tomu srov. např. Polčák, R. Internet Legal Culture, Lex Informatica and (un)Desired Sovereignty of Lawyers. In Lindskoug, P., Manusbach, U. Millqvist, G., Samuelsson, P., Vogel, H. H. Essays in Honour of Michael Bogdan. 1. vyd. Lund: Författarna och Juristförlaget i Lund, 2013, str. 477 a násl.

15 Srov. např. Fredland, J. S. Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies, Military Law Review, číslo 206, str. 26 a násl., nebo Brenner, S. Cyber-threats and the Limits of Bureaucratic Control, Minnesota Journal of Law, Science and Technology, roč. 14, číslo 1, str. 151 nebo též Grant, J. Will There Be Cybersecurity Legislation? Journal of National Security Law and Policy, roč. 4, str. 104. Další důvody zvláštního charakteru kybernetické bezpečnosti přidává Paul Rosenzweig v textu Rosenzweig, P. Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 390.

totiž zpravidla nemají hodnotu per se, ale závisí na tom, čemu v konečném důsledku slouží[16]. S trochou nadsázky tedy lze prohlásit, že tentýž router může sloužit jako součást informační infrastruktury internetové kavárny i atomové elektrárny, přičemž jeho bezpečnostní hodnota není dána jeho cenou, ale způsobem jeho užití[17].

Výjimkou ze shora uvedeného jsou systémy a sítě, jejichž smyslem a účelem je působit jako součást národní informační a komunikační infrastruktury. Typicky např. tzv. páteřní sítě neodvozují svoji důležitost od hodnoty funkcionalit, k nimž byly pořízeny, neboť jejich funkcí je udržovat v chodu informační síť jako takovou – v jejich případě tedy není nutno hodnotit, jakému primárnímu účelu slouží, neboť jejich důležitost je zpravidla dána faktory, jako jsou kapacita, zastupitelnost apod[18].

Druhým významným faktorem odlišujícím legislativní řešení kybernetické bezpečnosti od ostatních oborů platného práva je její procesní orientace. Zatímco právní úprava krizového řízení resp. úprava bezpečnosti kritických funkcionalit státu je tradičně postavena na objektovém principu, je kybernetickou bezpečnost nutno primárně vnímat jako ochranu informačních procesů[19]. Tomu pak musí odpovídat celá regulatorní logika i fungování příslušných orgánů veřejné moci, neboť primárním smyslem a účelem není ochrana existence nebo funkčnosti konkrétně definovaného objektu, ale zajištění bezproblémové existence informačních transakcí. Výsledné řešení přitom samozřejmě nemůže být vzhledem k objektům dohromady tvořícím naši

16 Srov. např. systematiku hrozeb dle Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace, Harvard Journal of Law and Technology, roč. 25, číslo 2, str. 445.

17 Srov. např. Shane, P. M. Cybersecurity Policy as if „OrdinaryCitizens" Mattered: The Case for Public Participation in Cyber Policy Making, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 435.

18 V českém právu je tato skutečnost zohledněna subsidiárním kritériem pro určení prvku kritické informační a komunikační infrastruktury ve smyslu ust. části VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

19 Srov. Hathaway, M. E., Klimburg, K. Preliminary Considerations: On National Cybersecurity, in Klimburg, A. National Cybersecurity – Framework Manual, Talinn: CCDCOE, 2012, str. 8.

informační a komunikační infrastrukturu absolutně indiferentní – objekt však má být předmětem regulatorního zájmu až v důsledku jeho konkrétní důležitosti pro kritický informační proces[20].

Třetím specifickým rysem právní úpravy kybernetické bezpečnosti je právní jev, který je doktrínou popisován jako fenomén definičních autorit. Veškeré lidské jednání totiž v prostředí informačních sítí neprobíhá bezprostředně, ale je zprostředkováváno službami informační společnosti. Člověk ani právnická osoba tedy nemůže v prostředí informačních sítí činit nic bez toho, aby se na jeho jednání fakticky nepodílela hned celá řada poskytovatelů služeb informační společnosti[21].

Označení definiční autority si tyto subjekty vysloužily z toho důvodu, že mají faktickou možnost definovat formou kódu (tzv. definiční normy) technické parametry jednání svých uživatelů. Nejedná se přitom o normu právní, neboť poskytovatelé služeb informační společnosti nedisponují právotvornou kompetencí (jde povětšinou o soukromé subjekty)[22] – přesto jde nepochybně o pravidlo, které má na jednání uživatelů zásadní vliv.

Definiční charakter těchto technických resp. faktických pravidel je od právních norem odlišuje i co do jejich fungování. Byť jde o pravidla vytvořená člověkem a zaměřená k regulaci lidského chování, nemají charakter povinnostní, ale jde o kauzální normy přímo determinující na technické úrovni

20 Viz např. Srov. např. Lin, H. Thoughts on Threat Assessment in Cyberspace, Journal of Law and Policy for the Information Society, roč. 8, číslo 2, str. 338. Současná česká právní úprava je naproti tomu vzhledem ke kritické informační a komunikační infrastruktuře orientována objektově. Je to dáno skutečností, že definiční kritéria pro kvalifikaci informačního systému nebo sítě obsažená v části VI.G.a., VI.G.b. a VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb. jsou svázána s objektovými definicemi ostatních prvků národní kritické infrastruktury.

21 Základem teorie definičních autorit je práce amerického konstitucionalisty Lawrence Lessiga op. cit. v pozn. 6. Z českých pramenů viz např. Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 137 a násl.

22 K institucionálním požadavkům na právotvůrce viz např. Kelsen H. Pure Theory of Law, přel. Paulson, B. L., Paulson S., Oxford: Oxford University Press, str. 91 a násl.

výsledek lidského jednání[23]. Jsou to v podstatě člověkem vytvořené normy zaměřené k regulaci lidského chování, ale jejich technický charakter jim dává povahu kauzálního přírodního zákona.

Z právního hlediska jde o extrémně zajímavý jev mající zásadní dopady především do problematiky odpovědnosti za protiprávní jednání[24]. Především z toho důvodu, že poskytovatelé služeb informační společnosti jsou v problematických případech jedinými subjekty, které lze reálně nalézt, proti nimž lze uplatnit právní postih a které jsou technicky schopny problematickou situaci efektivně řešit, vznikla celá relativně samostatná teorie spoluodpovědnosti těchto poskytovatelů za protiprávní jednání jejich uživatelů[25]. Dokonce lze konstatovat i dříve nevídaný obecný trend přesouvat vymáhání subjektivních práv od jejich skutečných rušitelů (tj. od individuálních uživatelů) právě k poskytovatelům služeb, jejichž prostřednictvím k porušování těchto práv dochází, respektive která protiprávní jednání technicky zprostředkovávají[26].

V oblasti kybernetické bezpečnosti se fenomén definičních autorit rovněž projevuje zásadním způsobem, a to osobní působností příslušných právních předpisů. Povinnosti plynoucí z potřeby chránit kritické informační

23 Namísto povinnosti v tomto případě hovoříme o nutnosti člověka jednat určitým způsobem. Definiční norma nepůsobí nutnost jednat pouze v situaci, pokud ji její adresát dokáže technicky eliminovat. Definiční normou tedy není vázán pouze hacker (v pravém smyslu toho slova) – viz Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 193.

24 Ve státech Evropské unie vznikla za tímto účelem specifická legislativa omezující odpovědnost poskytovatelů služeb informační společnosti za protiprávnost jednání jejich uživatelů. Harmonizačním předpisem je směrnice 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), přičemž do českého práva byla omezení implementována zákonem č. Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

25 Obsáhlé zmapování aktuální české, slovenské i zahraniční rozhodovací praxe přináší publikace Husovec, M. Zodpovednosť na internete podľa českého a slovenského práva, Praha: CZ.NIC, 2014, ke stažení on-line na adrese http://knihy.nic.cz/files/nic/edice/Zodpovednost_web_FINAL.pdf.

26 Důsledkem tohoto trendu jsou naneštěstí i některé extrémní právní konstrukce, jako např „třikrát a dost" v zákoně HADOPI – srov. např. working paper Dejean, S., Pénard, T., Suire, R. Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, Rennes: CREM, ke stažení on-line na adrese http://www.01net.com/genere/article/fichiersAttaches/300415066.pdf.

funkcionality státu resp. národní informační a komunikační infrastrukturu nejsou v tomto případě vůbec ukládány koncovým uživatelům, ale směřují ve velké míře na poskytovatele služeb resp. na správce zájmových systémů a sítí[27].

V tomto směru je možno vidět i další podstatný rozdíl mezi právní úpravou krizového řízení a kybernetickou bezpečností, neboť v případě krizového řízení může právní úprava bezprostředně dopadat na libovolné fyzické či právnické osoby. Rozsah osobní působnosti právní úpravy kybernetické bezpečnosti naproti tomu nepočítá s dopadem na nikoho jiného, než jsou právě poskytovatelé služeb - v případě české právní úpravy jde konkrétně o poskytovatele služeb elektronických komunikací[28].

Posledním základním rysem právní úpravy kybernetické bezpečnosti, který z ní činí specifický regulatorní fenomén, je značná míra konvergence soukromého a veřejného zájmu. Obecně bývá obvyklé, že v případě zájmu

27 Správcem je pro potřeby zákona č. 181/2014 Sb. analogicky s definicí obsaženou v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, subjekt, který určuje účel provozu příslušného informačního systému nebo sítě – povinnosti pak zákon stanoví právě jemu. K tomuto přístupu viz např. Berejka, M. A Case for Government Promoted Multi-Stakeholderism, Journal on Telecommunications and High-Tech Law, roč. 10, str. 9.

28 Takto široký rozsah působnosti zákona uplatní se navíc pouze ve výjimečném případě vyhlášení stavu kybernetického nebezpečí. Za standardní situace běžného fungování systému národní kybernetické bezpečnosti mají konkrétní zákonné povinnosti pouze správci zvlášť určených systémů a sítí (poskytovatelé služeb elektronických komunikací mají pouze povinnost hlásit své kontaktní údaje). K tomu viz § 3 zákona č. 181/2014 Sb., přičemž zákonné povinnosti nad rámec hlášení kontaktních údajů jsou dalšími ust. ukládány pouze subjektům vypočteným v § 3 písm. c) až e) zákona č. 181/2014 Sb. – srov. zejm. § 4 odst. 1 a 2 zákona č. 181/2014 Sb.

na ochraně tzv. nedistributivních[29] práv je výsledná právní úprava konfliktní se soukromým zájmem resp. s distributivními právy osob[30]. Vzájemné vyvážení soukromého a veřejného zájmu je v takových případech nezřídka otázkou právní a politické alchymie[31]. Pokud však má právní úprava nedistributivního práva jako v případě českého zákona o kybernetické bezpečnosti pouze nezbytně nutný věcný rozsah, je hodnotově konzistentní s tím, co lze označit za tvrdé jádro ústavy[32], a navíc má na distributivní práva jen minimální dopad. Tím dochází k výjimečně nekonfliktní situaci[33].

Jestliže tedy můžeme konstatovat, že naše právní úprava kybernetické bezpečnosti není zásadně konfliktní ve vztahu k distributivním právům, je to dáno především skutečností, že omezení, která reálně přináší, jsou v porovnání s důležitostí chráněných zájmů jen nepatrná. Nejzávažnějším bezprostředním zásahem do distributivních práv je v tomto případě zásah do práva vlastnického, neboť povinným subjektům může vzniknout povinnost investovat své prostředky do zabezpečení vlastní informační a komunikační infrastruktury.

Jak vyplynulo z jednání vedoucích k přijetí zákona o kybernetické bezpečnosti, jsou tyto investice již standardně povinnými subjekty realizovány – nikoli

29 Pojem distributivnosti práv je výtečně vyložen v odlišném stanovisku Pavla Holländera k nálezu pléna Ústavního soudu ze dne 3. 4. 1996, č. j. Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215, dostupné z: www.nalus.usoud.cz, následovně: „Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků (public goods, kolektive Gütter). Rozdíl mezi nimi spočívá v jejich distributivnosti. Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným 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. (-) Pro základní práva a svobody je, na rozdíl veřejných statků, typická jejich distributivnost. Aspekty lidské existence, jakými jsou např. osobní svoboda, svoboda projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd., lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům."

30 V obecné rovině se tomuto fundamentálnímu konfliktu věnuje např. Ronald Dworkin v práci Dworkin, R. Justice for Hedgehogs, London: Belknap Press, 2011.

31 Z institucionálního hlediska se tomuto problému věnuje např. text Kelly, T. K., Hunker, J. Cyber Policy: Institutional Struggle in a Transformed World, I/S: Journal of Law and Policy, roč. 8, číslo 2, str. 210 a násl.

32 K pojmu viz např. Höllander, P. Materiální ohnisko ústavy a diskrece ústavodárce, Právník, roč. 2005, č. 4, str. 318.

33 Viz Powell, B. Is Cybersecurity a Public Good? Evidence From the Financial Services Industry, Journal of Law, Economics and Policy, roč. 1, číslo 2, str. 497.

sice z důvodu jejich zájmu na zajištění národní kybernetické bezpečnosti, ale z čistě zištného zájmu na ochraně vlastních systémů před kybernetickými bezpečnostními incidenty. Ve většině případů tedy bude nutno ze strany povinných subjektů investovat pouze do komponent zajišťujících komunikaci s národním nebo vládním CERT resp. dokumentaci odpovídající zákonnému standardu[34].

1.3 Principy české a evropské právní úpravy kybernetické bezpečnosti

V právu EU je specifická právní úprava kybernetické bezpečnosti v současné době ve stadiu implementace základních normativních právních aktů[35], zatímco v České republice je komplex zákona a podzákonných normativních právních aktů již účinný. Přestože vznikala nezávisle na sobě, sdílejí obě legislativní řešení stejnou regulatorní strategii a z jejich struktury lze rovněž vyčíst prakticky obdobný systémový základ. Důvodová zpráva k zákonu o kybernetické bezpečnosti shrnuje tyto principy následovně[36]:

- Princip technologické neutrality[37] – na základě toho principu, jehož jedním z rozměrů je i tzv. síťová neutralita, dochází ke striktnímu oddělení obsahu komunikace od technologií používaných pro jeho ukládání nebo přenos. Informační a komunikační technologie jsou tedy neutrální vzhledem ke způsobu, kterým jsou používány.

34 Není v tomto směru žádným tajemstvím, že naše podzákonná úprava konkrétních náležitostí bezpečnostních opatření a jejich dokumentace vychází ze široce akceptovaného standardu organizačních norem v oblasti informační bezpečnosti z rodiny ISO 27k. Kritickou analýzu těchto standardů viz např. v příspěvku Vorobiev, V. I., Fedorchenko, L. N., Zabolotsky, V. P., Lyubimov, A. V. Ontology-based analysis of information security standards and capabilities for their harmonization, in Proceedings of the 3rd international conference on Security of information and networks, New York: ACM, 2010, str. 137 a násl.

35 Viz zejm. směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

36 Ze srovnání např. se strategií legislativy ke kybernetické bezpečnosti USA plynou základní rozdíly právě ve volbě jejích určujících principů – relativně větší úspěch českého resp. evropského legislativního přístupu ukazuje, že tento zřejmě více odpovídá aktuálnímu stavu politického a společenského diskursu. K tomu srov. např. Grant, J. Will there Be Cybersecurity Legislation? Journal of National Security Law & Policy, roč. 4, str. 103 a násl.

37 K původnímu významu tohoto pojmu viz např. Balabanian, N. Presumed Neutrality of Technology, Society, roč. 17, číslo 3, str. 7.

Důležitým aspektem technologické neutrality je rovněž nezávislost právního regulačního rámce na konkrétní technologii – právní regulace je tedy důsledně neutrální vůči produktům různých dodavatelů (žádný z nich nepreferuje ani nevylučuje).

- Princip ochrany informačního sebeurčení člověka[38] – informační sebeurčení člověka zahrnuje nejrůznější základní informační práva, z nichž pro kybernetickou bezpečnost jsou důležité především právo na ochranu soukromí, právo na ochranu osobních údajů, právo na svobodný přístup k informacím a právo na přístup ke službám informační společnosti (to vychází ze skutečnosti, že v dnešní době nelze žít plnohodnotný soukromý život bez toho, aby měl člověk možnost tyto služby využívat)[39].
- Princip ochrany nedistributivních práv[40] – v tomto případě jde především o ochranu národní bezpečnosti a specificky pak o ochranu bezpečnosti prostředí, v němž dochází k realizaci informačních transakcí (k tomu podrobněji viz dole).
- Princip minimalizace státního donucení – v případě návrhu právní úpravy jde především o implementaci výstupního kritéria třetího prvku testu proporcionality[41], v němž je nutno hodnotit, zda je zásah do lidské svobody proveden jen v nezbytně nutné míře. Konkrétně jde o svobodu povinných subjektů volně užívat předmět jejich vlastnického práva (tj. jejich informační a komunikační infrastrukturu). Ve vztahu k člověku se návrh v tomto směru omezuje prakticky dokonale, neboť

38 Dokonce i v odborné literatuře převažuje přesvědčení, že kybernetická bezpečnost je v kontrapozici k základním informačním právům – srov. např. Nojeim, G. T. Cybersecurity and Freedom on the Internet, Journal of National Security Law & Policy, roč. 4, str. 118 a násl. Ve skutečnosti je však ochrana základních práv jediným skutečným a legitimním smyslem a účelem kybernetické bezpečnosti. To mimo jiné reflektuje i aktuální praxe a agendě ochrany základních práv Valného Shromáždění OSN – srov. např. zprávu Zvláštního zpravodaje Valného shromáždění OSN č. A/HRC/17/27 – stejný názor ve vztahu k právu na soukromí viz např. v článku Bambauer, D. Privacy versus Security, The Journal of Criminal Law & Criminology, roč. 103, číslo 3, str. 667.

39 Podrobněji viz Polčák, R. Internet a proměny práva, Praha: AUDITORIUM, 2012, str. 326.

40 Srov. Powell, B. J. Is Cybersecurity a Public Good? Evidence from the Financial Services Industry, Journal of Law, Economics and Policy, roč. 1, číslo 2, str. 497 a násl.

41 Do našeho právního řádu byl tento test zaveden kontinuální řadou rozhodnutí Ústavního soudu, z nichž můžeme vybrat rozhodnutí ze dne 12. 10. 1994, sp.zn. Pl. ÚS 4/94 nebo ze dne 21. 3. 2002, sp.zn. III. ÚS 256/01. K pojmu a metodě viz též např. viz Alexy, R. On the Structure of Legal Principles. Ratio Iuris. 2000, roč. 13, č. 3, str. 1 a násl. nebo Holländer, P. Filosofie práva. Plzeň: Aleš Čeněk, 2006, str. 158 a násl.

uživatelům služeb informační společnosti vůbec nezasahuje do jejich práv (zákon se netýká informačních práv uživatelů, nezasahuje do jejich soukromí ani jim neukládá žádná jiná omezení či povinnosti).

- Princip autonomie vůle regulovaných subjektů – tento princip se týká metody právní regulace a projevuje se stanovením cílových parametrů bez toho, aby právotvůrce nutil regulované subjekty k nějakému specifickému konkrétnímu řešení (subjekty si tedy volí způsob, jak cílového stavu dosáhnout v podmínkách, v nichž samy působí).
- Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství – tento princip označovaný v mezinárodním právu veřejném jako due dilligence[42] týká se odpovědnosti státu za mezinárodně škodlivé následky jednání, k němuž dojde pod jeho suverénní jurisdikcí (viz dále).

Za zvláštní pozornost stojí především princip ochrany nedistributivních práv směřující především k ochraně infrastruktury tvořené službami informační společnosti. Nedistributivní charakter bezpečnosti je v tomto případě dán skutečností, že tuto hodnotu nelze distribuovat, tj. nelze konstatovat, že z její existenci přímo plynou konkrétní práva jednotlivým subjektům. Namísto toho má bezpečnost celostní charakter (jde o ochranu prostředí jako celku) a práva k jeho ochraně vykonává výlučně stát podobně, jako je tomu např. v případě národní bezpečnosti nebo ochrany životního prostředí.

Je v tomto směru nutno zdůraznit, že bezpečnost obecně (tj. vč. kybernetické bezpečnosti) nepředstavuje hodnotu či relevantní zdroj legitimity právních norem sama o sobě. Jedná se jako u ostatních nedistributivních principů o akcesorický institut, jehož legitimita není dána přímo ale prostřednictvím primárních principů, k jejichž ochraně směřuje. Nelze tedy hovořit pouze o bezpečnosti bez dalšího resp. nelze jí per se odůvodňovat vznik nových právních povinností nebo obecně jakékoli zásahy do svobody člověka. Bezpečnost jako taková pak nemůže být ani ve struktuře proporcionality přímo poměřována s ostatními (distributivními) právními principy jako např. s právem na vlastnictví, právem na svobodu projevu nebo právem

42 Srov. Hessbruegge, J. A. The Historical Development of the Doctrines of Attribution and Due Dilligence in International Law.

na práci. Namísto toho je třeba vždy řešit otázku, co je bezpečností chráněno, tj. jaká primární hodnota resp. jaký primární princip je příslušnými konkrétními bezpečnostními instituty zajištěn[43].

Dominantním motivem české právní úpravy je tedy v tomto směru právo na informační sebeurčení[44]. To vychází genericky z práva na soukromý život, tj. práva člověka na osobní existenci, a to vzhledem k vlastní integritě (důstojnosti) i možnostem zapojení do společnosti. Komponentou informačního sebeurčení, která s rostoucí penetrací běžného života službami informační společnosti nabyla na zásadní důležitosti, je ochrana soukromí, z níž se ještě v poslední době specificky vydělila ochrana osobních údajů[45]. Bezpečnost této pasivní komponenty informačního sebeurčení má především charakter jistoty člověka ohledně rozumné míry zabezpečení soukromé informační sféry před násilnými vnějším vlivy.

Aktivní komponentou informačního sebeurčení, která má vzhledem ke kybernetické bezpečnosti přinejmenším srovnatelný význam jako ochrana soukromí a osobních údajů, je právo na komunikaci. Jeho podstatou je předpoklad, že člověk nemůže vést plnohodnotný soukromý život bez toho, aby měl možnost běžným způsobem interagovat s okolním světem, tj. především komunikovat

43 Ke smyslu kybernetické bezpečnosti jako ochrany informačních práv člověka viz např. Polčák, R. Vygum v kyberprostoru: Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z. Information Security Summit 2011. 1. vyd. Praha: Data Security Management, 2011, str. 159-165.

44 Pojem informačního sebeurčení byl do právní praxe zaveden rozhodnutím Ústavního soudu Spolkové republiky, které se týkalo připravovaného sčítání lidu a jehož předmětem bylo primárně proporcionální vymezení informačního soukromí člověka. Viz nález Spolkového ústavního soudu ze dne 15. 12. 1983, č. j. BVerfGE 65, 1 [on-line]. Dostupné z: <www.thm.de/datenschutz/images/stories/volkszaehlungsurteil_bverfger_1983.pdf>.

45 Srov. např. Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, 2006, str. 14. Pojmu soukromí se v českém právu věnuje jen minimum kvalitní doktrinální literatury – světlými výjimkami jsou např. sborník Šimíček, V. (ed.) Právo na soukromí. Brno: Mezinárodní politologický ústav, 2011 nebo monografie Matejka, J. Internet jako objekt práva – hledání rovnováhy autonomie a soukromí, Praha: CZ.NIC, 2013, k dispozici též on-line ke stažení na adrese https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

formou, která je v příslušných sociokulturních reáliích obvyklá[46]. V aktuálních podmínkách je tak tuto komponentu informačního sebeurčení možno přeložit jako právo na přístup k (fungujícím) službám informační společnosti[47].

Právě uvedené samozřejmě neznamená, že by stát měl povinnost zajistit všem subjektům dodávky služeb informační společnosti nebo že by uvedené služby měly být s garancí státu poskytovány bezplatně. Stát má však v situaci, kdy jsou tyto služby běžnou součástí soukromého lidského života, povinnost garantovat jejich dostupnost a na nejvyšší úrovni též jejich funkčnost. To v tomto případě mimo jiné znamená též povinnost státu zabezpečit tyto služby tak, aby mohly být poskytovány a konzumovány bez obav o jejich bezpečnost. Z právě uvedeného tedy plyne, že jen bezpečné služby informační společnosti mohou dát člověku prostor k nerušené realizaci jeho práva na informační sebeurčení.

S tím souvisí i jiný princip, který český návrh nijak zvlášť nezdůrazňuje, ale který má ve vztahu ke kybernetické bezpečnosti rovněž zásadní význam, tj. princip svobody projevu. Na rozdíl od informačního sebeurčení se v tomto případě jedná namísto aktivní soukromé komunikace o zabezpečení možnosti veřejně vyjádřit svůj názor a případně se účastnit obecného

46 Skutečnost, že soukromí člověka tvoří i možnost komunikovat s okolím, zdůraznil náš Ústavní soud, přičemž původně poukázal především na nutnost ochrany informačních vztahů v rámci rodiny. Doslova k tomu uvedl: „Právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob. Přílišná akcentace pozitivní složky práva na ochranu soukromého života vede k neadekvátnímu zúžení ochrany pouze na to, aby skutečnosti soukromého života fyzické osoby nebyly bez jejího souhlasu či bez důvodu uznávaného zákonem a tak nebyla narušována integrita vnitřní sféry, která je pro příznivý rozvoj osobnosti nezbytná. Ústavní soud nesdílí toto zúžené pojetí, neboť respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“ – viz nález Ústavního soudu ze dne 1. 3. 2000, č. j. II. ÚS 517/99, N 32/17 SbNU 229.

47 Ústavní soud se k této otázce vyjádřil v nálezu ze dne 07. 04. 2010, č. j. I.ÚS 22/10 následovně: „Lze dovodit, že člověk tak bývá netoliko objektem společenských ‚poměrů‘, ale stává se i objektem práva, je-li nucen podrobovat se mu zcela při jeho interpretaci a aplikaci, tj. bez zohlednění jeho individuálních zájmů, resp. základních práv. Vedle subjektivních faktorů na straně jednotlivce je při posuzování ‚obvyklosti, resp. oprávněnosti‘ výdaje třeba vzít v úvahu i faktory objektivní, mezi ty mimo jiné patří technologický vývoj (např. mobilní telefony, internet) a s ním související změny ve způsobech komunikace, získávaní informací, styku s úřady, sdružování apod., resp. vývoj technologií, skrze niž je realizováno právo jednotlivce na osobní rozvoj, vztahy s ostatními lidmi a vnějším světem, tedy právo na soukromý život.“

společenského nebo politického diskursu. Stejně jako v případě informačního sebeurčení je přitom možno konstatovat, že pouze bezpečně fungující služby informační společnosti mohou k takové účasti poskytnout adekvátní prostor[48].

Ostatní shora uvedené principy mají ve struktuře navrhované právní úpravy spíše implementační charakter. Princip technologické neutrality zdůrazněný hned na prvním místě týká se především skutečnosti, že česká právní úprava směřuje k zajištění funkčnosti informační a komunikační infrastruktury bez toho, aby se týkala komunikovaného obsahu[49]. Právní povinnosti subjektů ani pravomoci založené zákonem Národnímu bezpečnostnímu úřadu se tedy z podstaty nemohou týkat dat tvořících obsah komunikace prostřednictvím služeb informační společnosti. Dalším aspektem technologické neutrality je v tomto případě skutečnost, že povinné technické standardy ani technická řešení přímo implementovaná na národní úrovni nebudou zvýhodňovat nebo upřednostňovat žádnou konkrétní proprietální technologii[50].

Princip autonomie vůle regulovaných subjektů a princip minimalizace státního donucení vztahují se především k osobní působnosti, rozsahu a míře obecnosti konkrétních právních povinností definovaných právní úpravou. Ta je minimalistická v tom směru, že se vztahuje pouze na omezený okruh subjektů, přičemž míra zátěže těchto subjektů specifickými povinnostmi odpovídá důležitosti jimi spravovaných systémů a míře jejich bezpečnostní expozice.

Zohlednění maximální autonomie vůle při formulaci povinností pro subjekty spadající do osobní působnosti zákona má aspekt liberální i pragmatický.

---

48 Kybernetická bezpečnost se stala i jedním z ústředních motivů zprávy Zvláštního zpravodaje Valného shromáždění OSN k zásadním problémům práva na svobodu projevu – viz kap. IV., část E, Report of the Special Rapporteur on thepromotion and protection of the right to freedom of opinion and expression, Frank La Rue, č. A/HRC/17/27, ke stažení on-line na adrese www.ohchr.org.

49 K tomu srov. např. Yoo, C. S. Network Neutrality and the Economics of Congestion. Georgetown Law Journal, roč. 94, str. 1847 a násl.

50 K důležitosti tohoto principu vzhledem k fungování síťových efektů, na nichž je prakticky založen další rozvoj naší kultury v nejširším smyslu slova, viz např. Zittrain, J. The Generative Internet. Harvard Law Review, roč. 119, str. 1974.

Inkorporace tohoto principu je pro regulované subjekty přirozeně příznivá, neboť jim poskytuje maximální volnost při implementaci příslušných povinností.

Vedle toho tento princip zohledňuje i značnou rozmanitost informačních sítí a systémů, jichž se dotýká. Pokud by byla úprava rigorózní co do specifikace konkrétních povinností, znamenalo by to buďto definovat nespočet variant dle rozsahu a funkcí příslušných sítí a systémů nebo pracovat s předpokladem, že standardní zákonné varianty budou vyhovovat co do efektivity vynaložených investic pouze některým subjektům. To by v konečném důsledku vedlo na jedné straně k tomu, že by byly některé subjekty nuceny investovat prostředky do bezpečnostních opatření, která by byla vzhledem k charakteru příslušných systémů přehnaně rozsáhlá, a jiné subjekty by naopak ani při splnění zákonných požadavků neochránily svoji infrastrukturu v dostatečném rozsahu. Namísto toho volí zákon stanovení cílového stavu, tj. požadované úrovně funkčnosti bezpečnostních opatření, přičemž ponechává regulovaným subjektům relativní volnost ve volbě konkrétních nástrojů pro jeho dosažení. To ostatně odpovídá i jedné ze shora zmíněných komponent principu technologické neutrality, neboť zákonné podmínky lze splnit nespočtem typů různých bezpečnostních řešení založených na technologiích od různých vzájemně si konkurujících dodavatelů.

Druhým aspektem autonomie vůle je možnost dobrovolné spolupráce soukromoprávních subjektů stojících mimo osobní působnost zákona s národním dohledovým pracovištěm. Přestože se tato zákonná konstrukce jeví být na první pohled absurdní, lze o tuto formu spolupráce očekávat velký zájem především mezi subjekty, které jsou předmětem zvýšené bezpečnostní expozice, ať už jde o aktivistické útoky na jejich infrastrukturu, konkurenční boj, průmyslovou špionáž apod. Spoluprací s národním dohledovým pracovištěm mohou tyto subjekty získat nejen přehled o tom, jaká je v reálném čase bezpečnostní situace v české informační a komunikační infrastruktuře (a tím i schopnost reagovat na aktuální kybernetické hrozby v předstihu), ale mohou získávat i průběžnou metodickou a koordinační pomoc při řešení

kybernetických bezpečnostních incidentů. Nadto bude pro subjekty nabízející služby informační společnosti představovat dobrovolná spolupráce s národním dohledovým pracovištěm přidanou hodnotu, kterou budou moci prezentovat svým klientům.

Z hlediska povinných soukromoprávních subjektů však má inkorporace principu autonomie vůle též jeden problematický aspekt. Právní úprava totiž nepočítá s tím, že by měly povinnost nechat si ex ante schvalovat nebo nějak potvrzovat vlastní řešení kybernetické bezpečnosti vzhledem ke splnění standardních zákonných požadavků. Především u středních a velkých podniků a veřejnoprávních korporací investujících podstatné prostředky do rozvoje své informační a komunikační infrastruktury je přitom stěžejní otázkou tzv. compliance, tj. ex ante kontrolovaného plnění zákonných požadavků příslušné jurisdikce. Je totiž z ekonomického hlediska neúčelné pro tyto subjekty investovat do rozvoje vlastní infrastruktury určité prostředky a přitom nemít jistotu, že tyto investice negenerují nějaké právní riziko[51]. Skutečnost, že zákon ve své struktuře neobsahuje explicitní povinnost certifikace nebo jiného schválení příslušných technických a organizačních řešení tedy je na první pohled pro regulované subjekty příznivá, neboť jim nevznikají další náklady spojené se schvalovacími procesy. Středním a velkým povinným subjektům však může způsobit zvýšení míry rizikovosti jejich investic do informační a komunikační infrastruktury, neboť neposkytuje ex ante jistotu, že jimi implementovaná bezpečnostní řešení skutečně bezezbytku plní zákonné požadavky. Nabízí se samozřejmě řešení formou regresní odpovědnosti dodavatelů – takové řešení však již není otázkou compliance a pro střední a velké subjekty představuje jen těžko postižitelné právní a ekonomické riziko[52].

Princip bdělosti ve vztahu k mezinárodnímu společenství a ostatním suverénním státům se v navrhované právní úpravě projevuje už samotnou skutečností, že se Česká republika snaží při vynaložení podstatného úsilí dostat pod kontrolu bezpečnostní problémy vyskytující se pod její jurisdikcí.

---

51 Srov. Weill, P., Woodham, R. Don't Just Lead, Govern: Implementing Effective IT Governance. MIT Sloan Working Paper No. 4237-02, 2002, dostupné on-line na adrese http://ssrn.com/abstract=317319.

52 Podrobněji k tomuto problému viz dále.

Obecně totiž tento princip zakládá odpovědnost státu za škodlivé následky způsobené ostatním státům v důsledku porušení mezinárodního práva veřejného v situacích, kdy stát mohl takovému porušení zabránit.

V situaci, kdy je infrastruktury na území státu zneužito k provedení kybernetického útoku s dopady v zahraničí, mají postižené státy a mezinárodní společenství důvod ptát se, zda škodlivým následkům nebylo možno zabránit. Existují-li popsané způsoby, jak předejít kybernetickým útokům resp. zneužití informační a komunikační infrastruktury, a kdy je implementace nejrůznějších bezpečnostních opatření nejen technicky možná ale též ekonomicky a sociálně akceptovatelná, pak má stát typu České republiky nikoli pouze právo ale přímo povinnost řešit svou vlastní kybernetickou bezpečnost[53].

---

53 Tato doktrína je ještě na počátku svého vývoje, ale lze při mírném optimismu předpokládat její brzké uplatnění v praxi – viz Glennon, M. The Dark Future of International Cybersecurity Regulation, Journal of National Security Law and Policy, roč. 6, str. 563.

2 INSTITUTY ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Před výkladem k jednotlivým institutům je nutno vyjádřit se ke třem populárním mýtům vztahujícím se k právu kybernetické bezpečnosti. První z nich týká se smyslu a účelu specifické legislativy a je založen na předpokladu, že právní předpis upravující práva a povinnosti k zajištění národní kybernetické bezpečnosti má ve svém textu obsahovat pro jednotlivé zainteresované subjekty komplexní návod na to, jak se správně chovat respektive důkladný popis toho, co je zakázáno. Zvláštní zákon upravující oblast národní kybernetické bezpečnosti však nemá a ani nemůže sloužit jako kuchařka – namísto toho má pouze v minimální formě upravit specifické povinnosti povinným subjektům a dále pak založit kompetence institucím, do jejichž působnosti tato oblast spadá. Je přitom třeba vycházet nikoli z předpokladu, že všem zainteresovaným je třeba zákonem detailně a nekompromisně sdělit, co mají nebo nemají dělat, ale že:

- právo není jen zákon – konkrétní obsah zákonných povinností nebývá nutně specifikován pouze zákonem, ale může být též např. otázkou judikatury či aplikace obecných či zvláštních právních principů. Z toho mj. plyne i skutečnost, že zákon může zůstat relativně rigidní, ale obsah platného práva se může v čase výrazně měnit[54],
- soukromým subjektům mají být zákonem stanoveny pouze konkrétní příkazy nebo zákazy – dovolené jednání není třeba vymezovat, neboť tyto subjekty mohou činit vše, co jim zákon nezakazuje[55],
- orgánům veřejné moci má zákon vymezit působnost, stanovit povinnosti a možnosti autoritativního jednání (orgány veřejné moci mohou totiž oproti subjektům soukromého práva dělat jen to, co jim zákon výslovně ukládá nebo umožňuje)[56],
- není vhodné ani potřebné upravovat to, co upravují jiné právní předpisy nebo mezinárodní smlouvy resp. zakládat povinnosti, které jsou

54 Výmluvně to ilustruje Gustav Radbruch v článku Zákonné neprávo a nadzákonné právo původně publikovaným jako Radbruch, G. Gesetzliches Unrecht und übergesetzliches Recht, Süddeutsche Juristenzeitung, roč. 1946, str. 105–108.

55 Viz čl. 2 odst. 3 Listiny základních práv a svobod.

56 Viz čl. 2 odst. 2 Listiny základních práv a svobod.

již založené jinými částmi našeho právního řádu. Z toho plyne též obecná nutnost strukturovat a formulovat zákon tak, aby do systému platného práva nevnášel redundantní nebo nekoherentní prvky[57],

- předmětem zákona je právní povinnost a normativními modalitami jsou příkaz, zákaz a dovolení. Co z nějakého důvodu není možné nebo účelné definovat jako právní povinnost prostřednictvím některé z těchto modalit, nemá v psaném právu co pohledávat. Typickým příkladem jsou technické standardy nemající charakter právních povinností. Zákon konečně nesmí ani odporovat ústavnímu pořádku České republiky – žádná zákonem založená právní povinnost nesmí vybočovat z rámce proporcionality základních práv člověka a nedistributivních práv státu[58].

Z právě uvedeného mimo jiné vyplývá, že právní úprava kybernetické bezpečnosti České republiky není ani zdaleka tvořena jen zákonem o kybernetické bezpečnosti. Povinnosti při ochraně informační a komunikační infrastruktury totiž kromě něj zakládá i řada dalších součástí českého právního řádu. Následující výklad je zaměřen na instituty, které se z hlediska zajištění kybernetické bezpečnosti jeví jako nejdůležitější z pohledu povinných subjektů. Konkrétně se budeme věnovat otázkám

- bezpečnostních opatření
- protiopatření
- odpovědnosti za nedbalost a prevenčních povinností
- disciplinární odpovědnosti a disciplinárních povinností

2.1 Bezpečnostní opatření

Bezpečnostní opatření jsou základním kamenem zákona o kybernetické bezpečnosti a z operačního hlediska i jeho zdaleka nejdůležitější součástí[59].

57 V tomto případě jde o komponenty označované právní teorií jako tzv. materiální náležitosti právotvorby normativního typu. K náležitostem i technice české právotvorby viz např. Šín Z.: Tvorba práva. Praha: C. H. Beck, 2003.

58 Proporcionalita je metoda poměřování právních principů, přičemž charakter právních principů mají i všechna ústavně zaručená základní práva. K používání této metody v českém právním prostředí viz učebnici Holländer, P. Filosofie práva, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

59 Zákon je v § 4 odst. 1 vymezuje jako „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru".

Primárním účelem zákona totiž není řešení jednotlivých kybernetických bezpečnostních incidentů ale vytvoření prostředí, v němž jsou kritická informační a komunikační infrastruktura státu a další zájmové informační systémy a sítě preventivně chráněny tak, že pro ně žádná kybernetická bezpečnostní událost nepředstavuje bezpečnostní riziko.

Zákon sám zavádí povinným subjektům pouze základní povinnost mít bezpečnostní opatření v taxativně vymezených kategoriích, přičemž technické podrobnosti upravuje prováděcí předpis[60]. Zákon je postaven na dokumentačním modelu, tj. ukládá povinným subjektům povinnost především dokumentovat jednotlivé typy bezpečnostních opatření a následně pak dává právo Národnímu bezpečnostnímu úřadu kontrolovat, zda je dokumentace souladná nejen s konkrétními požadavky zákona a prováděcího předpisu, ale samozřejmě též s aktuální skutečností.

Smyslem bezpečnostních opatření je primárně vytvoření takových preventivních mechanismů, které povinným subjektům umožní vyrovnávat se autonomně k kybernetickými bezpečnostními událostmi (ať už jde o prevenci jejich samotného vzniku nebo o nástroje a mechanismy k jejich následnému pokrytí)[61]. Subsidiárně jsou pak bezpečnostní opatření formulována tak, aby jejich zavedení umožnilo efektivní fungování kybernetických bezpečnostních struktur na úrovni státu, tj. především národního a vládního dohledového pracoviště.

Systematickým problémem bezpečnostních opatření, kterému jsme se už stručně věnovali výše, je skutečnost, že jsou formulována jako technický a organizační standard, aniž by však zákon předpokládal existenci oficiálních certifikačních nebo jiných a priori procedur použitelných k verifikaci jejich kvality. Povinné subjekty tedy budou investovat do akvizic nebo úprav příslušných bezpečnostních řešení, aniž by měly možnost a priori ověřit, zda to, čím se snaží plnit zákonné požadavky, skutečně je nebo není v souladu se zákonem resp. s prováděcím předpisem.

60 Viz vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

61 Za tímto účelem dělí zákon bezpečnostní opatření na organizační a technická a ty pak dále specifikuje v ust. § 5 odst. 2 a 3.

2.2 Protiopatření

Protiopatřeními pro potřeby tohoto textu souhrnně nazýváme to, co zákon označuje jako „opatření" a dělí dle typu na varování, reaktivní opatření a ochranná opatření. Všechny typy protiopatření mají povahu vrchnostenské činnosti Národního bezpečnostního úřadu, přičemž varování má charakter informativní a zbývající dvě opatření mají formu závazných individuálních právních aktů resp. opatření obecné povahy.

Institut varování může se zdát na první pohled zbytečným, neboť jeho užití nepřináší bezprostřední imperativ ani riziko přímé sankce[62]. Jeho charakter však vystihuje typický efekt zákona o kybernetické bezpečnosti v otázkách odpovědnosti za kybernetické bezpečnostní incidenty. Zákon totiž ani u imperativních institutů nepřináší žádné přímé drakonické sankce, ale zavádí přímo nebo nepřímo nové typy právních povinností, jejichž neplnění může mít za následek vznik povinnosti nahradit škodu. Povinný subjekt tedy nemůže kalkulovat právní riziko plynoucí z nově založených zákonných povinností pouze ve vztahu k možné pokutě (ta je co do své výše spíše symbolická) ale též vzhledem k velmi neurčitému potenciálu škod, k nimž může dojít v důsledku zaviněného[63] i nezaviněného[64] kybernetického bezpečnostního incidentu.

V případě varování tedy Národní bezpečnostní úřad sice provádí pouze adresnou osvětu ohledně konkrétních bezpečnostních rizik, ta ale ve svém důsledku vede k prokazatelné informovanosti povinných subjektů. Zprostředkovaně tím přináší povinným subjektům možnost založení povinnosti nahradit škodu způsobenou tím, že na základě varování nepřijmou přiměřená opatření k zabránění vzniku kybernetických bezpečnostních incidentů nebo zmírnění jejich následků[65].

V typickém případě tedy bude Národní bezpečnostní úřad formou varování informovat o konkrétním bezpečnostním riziku (např. o tzv. bezpečnostní díře) – jestliže povinné subjekty nebudou na základě této informace za vynaložení přiměřeného úsilí na takto identifikované riziko reagovat

62 Viz § 12 ve spojení s § 25 zákona č. 181/2014 Sb.

63 Odpovědnost je v tomto případě založena na základě obecných ust. § 2910 a násl. zákona č. 89/2012 Sb., občanský zákoník.

64 V úvahu zde u podnikatelských subjektů připadá povinnost nahradit škodu způsobenou provozní činností na základě § 2924 zákona č. 89/2012 Sb.

65 K tomu srov. § 2901 zákona č. 89/2012 Sb.

(např. instalací záplat) a v důsledku toho dojde ke škodě u třetích osob, mohou třetím osobám povinné subjekty přímo odpovídat z titulu nesplnění prevenční povinnosti. Je-li pak v této situaci způsobena škoda i samotnému povinnému subjektu, může být shora popsaný nedostatek reakce na varování též důvodem pro pojišťovnu, aby odmítla nebo výrazně snížila hodnotu pojistného plnění.

Z hlediska povinných subjektů tedy přináší i na první pohled bezzubý institut varování nový typ právního rizika, které je a priori jen velmi těžko ohodnotitelné – čím větší je přitom povinný subjekt a čím více spravuje systémů spadajících pod rozsah zákona o kybernetické bezpečnosti, tím je toto riziko závažnější, a to co do své potenciální hodnoty i do míry nepředvídatelnosti svého výskytu. Dokonce lze s trochou nadsázky konstatovat, že s rostoucí velikostí můžeme sledovat u povinných subjektů klesající míru zájmu o přímé sankce zákona o kybernetické bezpečnosti (tj. o pokuty) a naopak rostoucí zájmovost nepřímých sankcí ve formě právě popsaného potenciálu povinností k náhradě škody resp. limitace pojistného plnění[66].

Další dva typy protiopatření již disponují v porovnání s varováním též přímou možností autoritativního vynucení. Zákon definuje jejich věcný rozsah velmi široce - prakticky jde o jakákoli opatření „k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem“[67]. V tomto směru ale nelze na rozdíl od některých bulvárních názorů uvažovat o tom, že by takto široce definovaná věcná působnost příslušných správních rozhodnutí nebo opatření obecné povahy dávala Národnímu bezpečnostnímu úřadu do rukou nějaký totalitní nástroj ke kontrole národní informační a komunikační infrastruktury. Vedle konkrétního omezení smyslem a účelem protiopatření (resp. reaktivních nebo ochranných opatření) je v tomto případě Národní bezpečnostní úřad standardně omezen působností zákona a dále pak obecnými principy správního práva, z nichž nejdůležitějšími jsou zřejmě principy dobré správy[68] a zákaz svévole.

66 K nim ještě přistupují jen těžko vyčíslitelné náklady spojené s případnou kontrolou a realizací adresně uložených opatření k nápravě ve smyslu § 24 zákona č. 181/2014 Sb.

67 Viz § 13 odst. 1 zákona č. 181/2014 Sb.

68 K pojmu viz např. Košičiarová, S. Princípy dobrej verejnej správy a Rada Európy, Bratislava: Iura Edition, 2012, 556 s.

V rovině ústavního práva pak je Národní bezpečnostní úřad omezen především judikatorní doktrínou tzv. omezeného testu proporcionality[69]. Národní bezpečnostní úřad má tedy implicitní povinnost vybrat pro příslušné reaktivní nebo ochranné opatření takovou alternativu, která bude povinné subjekty nejméně zatěžovat.

Imperativní protiopatření zákon dělí z hlediska jejich účelu na reaktivní a ochranná. První jmenovaný typ se uplatní v případech hrozícího nebo probíhajícího konkrétního kybernetického bezpečnostního incidentu. Tomu odpovídá i procesní charakteristika reaktivních protiopatření zahrnující ve správním právu spíše výjimečné instituty okamžité vykonatelnosti a absence odkladného účinku řádného opravného prostředku (v tomto případě rozkladu)[70].

Okamžitost a bezprostřednost imperativního účinku reaktivních protiopatření odpovídá jejich charakteru jakožto bezpečnostních nástrojů výkonné moci. Přestože bylo nutno z hlediska procesní formy dostát požadavkům správního práva na dokonalý proces autoritativní aplikace, je zřejmé, že v tomto případě nejde o klasickou exekutivní aplikaci práva, ale spíše o konkrétní vrchnostenský zásah vedoucí k pokrytí okamžité bezpečnostní hrozby. Připodobnit jej lze namísto jiných procesů, na jejichž konci stojí vykonatelné správní rozhodnutí (resp. opatření obecné povahy), spíše k okamžité akci bezpečnostní složky výkonné moci, tj. např. k fyzickému zásahu policie[71].

V tomto případě však z podstaty věci plyne, že Národní bezpečnostní úřad nemá možnost provést takový zásah autonomně[72]. Exekutivní reakce k zajištění národní kybernetické bezpečnosti tedy v tomto případě nemůže mít povahu přímé akce bezpečnostní složky státu, ale pouze vrchnostenského

69 Jako omezený test proporcionality označuje se výstupní část standardního testu proporcionality, která spočívá v hodnocení míry zásahu do zájmu chráněného právním principem. Platí přitom, že zásah do práv osoby nesmí být větší, než je vzhledem k okolnostem pragmaticky nutné – srov. Holländer, P. Filosofie práva, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

70 Srov. § 15 zákona č. 181/2014 Sb.

71 Nabízí se zde například srovnání s pravomocemi policie při zajišťování bezpečnosti chráněných prostorů, objektů a osob ve smyslu ust. § 48 odst. 4 zákona č. 273/2008 Sb., o Policii české republiky, ve znění pozdějších předpisů.

72 K tomu viz shora konstatovaný specifický rys kybernetické bezpečnosti spočívající ve zprostředkovanosti veškerých aktivit službami informační společnosti.

imperativu vedoucího k akci subjektu, o jehož informační systém nebo síť se jedná. Nemaje ve správním právu jiného použitelného institutu, sáhl tedy v tomto případě právotvůrce logicky po institutu správního rozhodnutí resp. opatření obecné povahy.

Ochranná opatření mají naproti tomu svou náturou blíže ke klasickému správnímu rozhodování resp. k vrchnostenské podzákonné normotvorbě, neboť jde o imperativy, jejichž implementace, lidově řečeno, až tak nehoří. Jejich podkladem jsou rovněž konkrétní kybernetické bezpečnostní incidenty, ale jejich smyslem a účelem není bezprostřední reakce, nýbrž zvýšení úrovně bezpečnosti příslušných informačních systémů a sítí[73]. Především v případech, kdy jsou ochranná opatření vydávána formou opatření obecné povahy neurčitému okruhu adresátů, je lze vlastně z funkčního hlediska považovat za doplněk podzákonného předpisu konkretizujícího obsah bezpečnostních opatření.

2.3 Odpovědnost za nedbalost a prevenční povinnosti

Přestože sám zákon o kybernetické bezpečnosti se tomuto typu odpovědnosti z pochopitelných důvodů vůbec nevěnuje, představuje pro povinné subjekty možnost odpovědnosti za vědomou či nevědomou nedbalost resp. za nesplnění prevenční povinnosti zřejmě nejsilnější právní motivační faktor k faktické realizaci bezpečnostních opatření.

Odpovědnost v tomto případě znamená nejen potencialitu povinnosti nahradit škodu způsobenou třetím osobám v důsledku nedbalosti nebo opomenutí preventivního zásahu, ale též srovnatelně důležité riziko krácení nebo ztráty nároku na pojistné plnění u škod na vlastním majetku[74] resp. na vlastní činnosti nebo i riziko subsidiární sankce za nesplnění povinnosti specificky regulovaného odvětví (např. v oblasti energetiky[75]).

73 Srov. § 14 zákona č. 181/2014 Sb.

74 K tomu viz zejm. ust. § 2800 odst. 2 zákona č. 89/2012 Sb.

75 Vedle pokut či opatření k nápravě může jít též o nebezpečí odnětí licence nebo jiného povolení k výkonu specifické činnosti – tuto možnost dává národním regulátorům úprava např. v oblasti energetiky nebo elektronických komunikací – srov. zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů) nebo zákon č. 127/2005 Sb, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

K právě uvedeným typům odpovědnostních důsledků lze ještě připočíst riziko prodlení v případech, kdy kybernetický bezpečnostní incident způsobí neschopnost povinného subjektu plnit jiné právní povinnosti. Typicky může například dojít k situaci, kdy má povinný subjekt povinnost dodávat svým odběratelům zboží nebo služby a v důsledku kybernetického bezpečnostního incidentu toho není po nějakou dobu schopen. Za předpokladu, že kybernetický bezpečnostní incident vedl k takovým důsledkům kvůli neschopnosti povinného subjektu splnit si zákonnou povinnost vyplývající ze zákona o kybernetické bezpečnosti, nebude se povinný subjekt moci bránit poukazem na tento incident proti nárokům třetím osob z vadného resp. pozdního plnění.

To samozřejmě neznamená, že by povinné subjekty měly důvod obávat se toho, že budou odpovídat za veškeré škody způsobené třetím osobám kybernetickými bezpečnostními incidenty, na nichž se bude nějakým způsobem podílet jejich nedostatečně zabezpečená informační a komunikační infrastruktura. Ani v případě, byla-li by škoda třetím osobám skutečně způsobena v důsledku zanedbání specifických povinností plynoucích ze zákona o kybernetické bezpečnosti (resp. z jeho imperativních institutů), nejednalo by se ze strany povinného subjektu zřejmě o povinnost výlučnou – tam, kde byla např. v důsledku nedbalosti povinného subjektu zneužita jeho infrastruktura k provedení kybernetického útoku, zkoumal by soud u povinného subjektu míru jeho zavinění resp. míru toho, jak se nedbalá realizace opatření k zajištění kybernetické bezpečnosti podílela na celkovém škodním dopadu příslušného kybernetického bezpečnostního incidentu[76].

Za připomenutí stojí v této souvislosti především typologie nedbalostního zavinění sestávající vedle vědomé (tj. hrubé – culpa lata) nedbalosti též z nedbalosti nevědomé (tj. lehké – culpa levis)[77]. Za zaviněné porušení právní povinnosti se tak považují nejen situace, kdy má povinný subjekt prokazatelně k dispozici informace o hrozícím nebezpečí a vlastní liknavostí nezabrání škodlivému následku, ale také případy, kdy povinný subjekt

76 V tomto případě je specifický charakter kybernetických bezpečnostních incidentů společně s charakterem účasti způsobené nedůslednou ochranou vlastního systému možno obecně považovat za okolnosti hodné zvláštního zřetele a je tedy důvod předpokládat, že povinnost nahradit škodu bude v tomto případě specifikována dle míry zavinění resp. dle míry účasti – k tomu viz § 2915 odst. 2, první věta zákona č. 89/2012 Sb.

77 Viz např. Knapp, V. Některé úvahy o odpovědnosti v občanském právu. Stát a právo I. roč. 1956, str. 66.

sice těmito informacemi objektivně nedisponuje, ale opatřit si je měl a mohl. Ve vztahu ke shora zmíněnému institutu varování to mimo jiné znamená, že ze strany povinného subjektu nebude možno namítat například nefunkčnost povinně sdělované kontaktní adresy nebo interní komunikační problémy v rámci organizace, kvůli kterým se informace o varování vydaném Národním bezpečnostním úřadem nedostane na správné místo.

Nedbalost nebo nesplnění prevenční povinnosti každopádně nemusí mít důsledky pouze soukromoprávní. Řada povinných subjektů působí v odvětví, která mají specifickou a často i poměrně rigorózní správní regulaci – příkladem může být energetika, bankovnictví, elektronické komunikace, tzv. jiné utility (odpadové hospodářství, distribuce vody apod.), zdravotnictví nebo potravinářství. Ve většině z těchto odvětví mají povinné subjekty nejen povinnosti vztahující se bezprostředně k příslušnému typu činnosti, ale též související povinnosti, z nichž podstatná část se může přímo nebo nepřímo týkat provozu vnitřních informačních systémů nebo komunikačních sítí. Pokud v takovém případě dojde k narušení regulované činnosti povinného subjektu v důsledku kybernetického bezpečnostního incidentu, který povinný subjekt nedokázal zvládnout kvůli nedbalosti nebo porušení prevenční povinnosti, může to pro něj znamenat vedle shora uvedených odpovědnostních rizik též možnost postihu dle specifických pravidel příslušného regulovaného odvětví. Není pak v tomto směru žádným tajemstvím, že např. pro subjekty v oboru energetiky může být takový subsidiární sankční postih dle energetického zákona nepoměrně citelnější, než primární sankce plynoucí ze zákona o kybernetické bezpečnosti.

Všechna shora uvedená právní rizika jsou v porovnání s imperativními a sankčními mechanismy zákona o kybernetické bezpečnosti pro povinné subjekty nejen mnohem závažnější, ale také co do svého důsledku mnohem méně předvídatelná. Zatímco lze vcelku snadno odhadnout, jaká výše pokuty hrozí při neprovedení reaktivního protiopatření, jen těžko se dá z pohledu povinného subjektu odhadovat, jaký dopad může mít tatáž situace z pohledu soukromoprávní odpovědnosti vůči poškozeným třetím osobám, jak velká vymahatelná škoda může vzniknout zákazníkům nebo jak bude reagovat regulátor příslušného specifického odvětví (např. Energetický regulační úřad, český telekomunikační úřad apod.).

Velká míra této subsidiární právní rizikovosti ve spojení s absencí oficiálních compliance procedur vytváří na povinné subjekty tlak projevující se v důsledku jednak chvályhodnou vůlí investovat do bezpečnostních opatření, to dokonce často i vysoko nad rámec zákonných požadavků. Kromě toho však může tato nejistota vést k tomu, že se povinné subjekty budou za každou cenu snažit o únik z osobního rozsahu zákona nebo se budou pokoušet o různé ohýbání jeho pravidel. Zabránit tomuto efektu by kromě nezávislých certifikačních procedur mohla též osvětová činnost Národního bezpečnostního úřadu realizovaná ve spolupráci s odvětvovými regulátory nebo rozšíření nabídky pojistných či zajišťovacích finančních produktů. Svou nezastupitelnou roli pak budou jistě hrát i odvětvové organizace, které mohou vedle zprostředkování komunikace mezi povinnými subjekty a Národním bezpečnostním úřadem působit i v rovině vzdělávací, koordinační nebo poradenské.

2.4 Disciplinární odpovědnost a disciplinární povinnosti

Shora diskutovaná bezpečnostní opatření mají vést k tomu, že povinné subjekty budou mít systematicky řešenu kybernetickou bezpečnost tak, aby kybernetické bezpečnostní incidenty buďto nevznikaly nebo aby jejich výskyt neznamenal bezpečnostní riziko. Nástroje, s nimiž bezpečnostní opatření počítají, lze z pohledu platného práva rozdělit do následujících základních skupin:

- Technické prvky (specifický software a hardware vč. detekčních systémů, reportovacích nástrojů, autentizačních či kryptografických nástrojů, technika k zajištění fyzické bezpečnosti apod.)
- Analytické prvky a dokumentace (typicky analýza informačních aktiv, topografie sítí, analýza rizik apod.)
- Interní předpisy (organizační opatření, školící plány, krizové plány, interní instrukce pro vybrané skupiny zaměstnanců, interní pravidla pro nákup a outsourcing ICT apod.)
- Lidské zdroje (specificky vyčleněný personál k zajištění realizace bezpečnostních opatření nebo personál zajišťující výjimečně ad hoc určité činnosti v oblasti kybernetické bezpečnosti)

Poslední dvě uvedené kategorie týkají se vztahu povinného subjektu a jeho pracovníků, ať už jde o zaměstnance nebo obdobně působící externisty. Běžné fungování specificky vyčleněného personálu nebo pracovníků, jimž mohou být úkoly v oblasti kybernetické bezpečnosti ukládány ad hoc, jsou pro existenci a efektivitu bezpečnostních opatření kriticky důležité. Sebelépe postavený a vybavený bezpečnostní systém totiž není k ničemu, pokud není adekvátně obsluhován, resp. pokud jeho fungování brání faktická bezpečnostní rizika představovaná vlastními pracovníky povinných subjektů.

Z právního hlediska jde především o otázku povinností, které pracovníkům povinných subjektů ukládá zákon resp. povinností, které na základě zákona svým pracovníkům ukládají povinné subjekty formou interních instrukcí nebo běžné řídící činnosti v rámci korporátní hierarchie[78]. V tomto směru je předně nutno rozlišovat mezi pracovníky, jejichž pracovní náplň souvisí s tvorbou nebo realizací bezpečnostních opatření a pracovníky, jimž jsou pouze na základě bezpečnostních opatření ukládány konkrétní povinnosti s tím, že jejich běžná pracovní náplň s kybernetickou bezpečností jinak nesouvisí (tj. uživatele).

Bezpečnostní personál nebo pracovníky, u nichž alespoň část běžné pracovní agendy představuje kybernetická bezpečnost, lze logicky zatížit nejen větším množstvím pracovních povinností oblasti kybernetické bezpečnosti, ale lze od nich požadovat i vyšší míru odborné erudice a schopnosti plnit specifické požadavky interních bezpečnostních předpisů. Bezpečnostnímu technikovi, správci sítě nebo systémovému administrátorovi tak lze nejen uložit řadu specifických pracovních povinností, jejichž předmětem může být zabezpečení příslušné informační a komunikační infrastruktury, ale tyto povinnosti lze na úrovni interních předpisů nebo individuálních řídících aktů (tj. v rámci běžného podnikového řízení) formulovat i s vysokou mírou odbornosti a spoléhat přitom na adekvátní předvědění.

78 Rozdíl mezi interní instrukcí a aktem řízení spočívá v tom, že zatímco interní instrukce je určena neurčitému okruhu pracovníků splňujících určitou podmínku (např. pracovníkům v určité funkci), je akt řízení adresován, tj. určen konkrétnímu člověku. K povaze interní instrukce viz např. Galvas, M. a kol. Pracovní právo. Brno: Masarykova univerzita, 2012, str. 50 nebo Vysokajová, M. Zákoník práce - komentář. Praha: Wolters Kluwer, 2012, str. 623.

U profesí, jejichž pracovní náplň netvoří obsluha informačních technologií, je naproti tomu v případě definice povinností týkajících se bezpečnosti informačních systémů a sítí nutno postupovat tak, aby interní instrukce nebo jiné akty řízení byly obecně srozumitelné a aby byly z pohledu běžného pracovníka technicky proveditelné. Z toho plyne, že například instrukce typu „uživatel je povinen měnit své přístupové heslo minimálně jednou týdně, heslo musí mít min. 15 znaků, z nichž min. 7 znaků musí být speciální znaky ASCII" je vadná hned ze dvou důvodů. Jednak není možno rozumně požadovat po běžném uživateli, aby si každý týden zapamatoval nové patnáctiznakové heslo a navíc nelze předpokládat, že bude poučen v tom smyslu, co to jsou speciální znaky ASCII. Takto formulovaná interní instrukce tedy, byť její přečtení příslušný zaměstnanec potvrdí třeba podpisem vlastní krví, nikdy nepovede k právně vynutitelnému závazku.

Z právě uvedeného plyne, že problém disciplinární odpovědnosti zaměstnanců vzhledem k bezpečnostním opatřením zaváděným u povinných subjektů mandatorně na základě zákona o kybernetické bezpečnosti spočívá primárně ve způsobu, kterým budou různým kategoriím pracovníků ukládány příslušné bezpečnostní povinnosti. Neexistuje přitom žádná konkrétní judikatura, o kterou by bylo možno se opřít, to i přes skutečnost, že typově podobná situace jako v případě kybernetické bezpečnosti objevuje se dlouhodobě například v oblasti protipožární ochrany nebo bezpečnosti práce. Případy, jejichž autoritativní řešení máme k dispozici jako vodítko, týkají se spíše frapantních porušení interních předpisů nebo jiných řídících aktů a neposkytují tím pádem adekvátní návod pro diskutabilní či hraniční případy. Ještě žádného zaměstnavatele tak doposud nenapadlo například žalovat o náhradu škody zaměstnance, který, byť byl proškolen v použití hasicího přístroje, vzal raději před požárem v odpadkovém koši nohy na ramena.

Problematika závaznosti respektive míry závaznosti interních instrukcí na úseku kybernetické bezpečnosti každopádně představuje zajímavé a vysoce žádoucí zadání, jehož řešením se česká právní věda již intenzivně zabývá[79] – přestože by ale měly být základní doktrinální poznatky k těmto

79 Viz např. aktuálně řešený projekt GAMU MUNI/M/1052/2013, Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky.

otázkám k dispozici v řádu měsíců či jednotek let, budou povinné subjekty vystaveny právní nejistotě až do doby, kdy bude k dispozici adekvátní judikatura vyšších soudů.

Na tomto místě je nutno připomenout, že právě uvedené týká se pouze specifických bezpečnostních povinností, jejichž existence je podmíněna zvláštní autoritativní informací prokazatelně sdělenou zaměstnanci. Zaměstnavatel však samozřejmě nemusí zaměstnanci formou interních instrukcí nebo jiných řídících aktů sdělovat všechny možné požadavky na bezpečné fungování informačních systémů a sítí. Každé pracovní pozici totiž odpovídá implicitně předpokládaná odborná výbava zaměstnance, s níž zaměstnavatel může počítat a kterou nemusí ani zvlášť ověřovat.

Pracovní pozice, u níž se předpokládá znalost práce s osobním počítačem, tedy implicitně předpokládá, že bude zaměstnanec bez dalšího chápat například zákaz psaní přístupových hesel na žluté lístečky a jejich lepení na okraj monitoru (podobně není nutno kancelářské síly školit například v tom, že nemají strkat kancelářské sponky do elektrických zásuvek nebo v pracovní době skákat z oken). Analogicky pak bude zřejmě možno ze strany zaměstnavatele i bez nutnosti přijímat interní instrukce předpokládat, že systémový administrátor je obeznámen se skutečností, že nesmí používat triviální heslo nebo že se má při každém odchodu od počítače odhlásit ze své virtuální identity. Ani v těchto otázkách však nemáme k dispozici žádnou použitelnou judikaturu a vyjma evidentních případů lze spíše předpokládat, že soudy nebudou příliš respektovat presumpci nedbalostního zavinění a budou spíše v případě sporu požadovat po zaměstnavateli důkaz skutečnosti, že zaměstnanec příslušné bezpečnostní pravidlo znát mohl a hlavně, že jej vzhledem ke svému pracovnímu zařazení znát měl[80]. Podrobněji se typologii a praktickým otázkám závaznosti interních instrukcí věnujeme v následující kapitole.

[80] K tomu ještě přistupuje podstatný rozdíl mezi interní instrukcí a právním předpisem nebo vrchnostenským aktem spočívající v tom, že interní instrukce se nemůže spoléhat na presumpci správnosti resp. presumpci platnosti – srov. Bělina, M. a kol. Pracovní právo. 5. dopl. a podstat. přeprac. vyd., Praha: C. H. Beck, 2012, str. 66.

3 INDIVIDUÁLNÍ ODPOVĚDNOST ZA KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT[81]

3.1 Kybernetická bezpečnost jako agenda výkonné moci

Přestože informační nebo počítačová bezpečnost jsou tradičními tématy aplikované kybernetiky, představuje kybernetická bezpečnost relativně nový společenský fenomén. Tento primárně regulatorní koncept totiž nemá technickou podstatu, ale jedná se o komplex kvalitativně nových veřejnoprávních pravidel, jehož účelem je zajistit bezpečné fungování služeb informační společnosti[82].

Bezpečnost je pro informatiku nebo organizační disciplíny dostatečně solidním účelem, o který lze bez dalšího opřít vývoj nebo nasazení nejrůznějších technických či organizačních nástrojů. Pro právo, poučené relativně nedávnou historickou zkušeností, však bezpečnost nemůže představovat legitimní cíl, který by per se dokázal ospravedlnit regulatorní zásahy do lidské svobody. Praktické zkušenosti s nacistickým a komunistickým právem, tj. s řády pravidel postavenými na nenávistné ideologii, nás totiž donutily ptát se nikoli pouze na to, zda příslušná právní povinnost povede k vyšší míře bezpečnosti, ale též k čemu nebo pro koho má taková bezpečnost sloužit. Vedle hlediska efektivity nás tedy v právu musí vždy a nutně zajímat též otázka fundamentální legitimity bezpečnostních řešení[83].

Bezpečnostní pravidla bývají v porovnání s ostatními částmi právního řádu co do míry zásahu do lidské svobody poměrně razantní. Jejich podstata je navíc postavena na předpokladu, že řešení bezpečnostně exponovaných situací nemůže být otázkou měsíců či let, ale že komplex bezpečnostních nástrojů musí být nastaven tak, aby k jejich užití mohlo dojít v bezprostředním důsledku bezpečnostní hrozby nebo dokonce i preventivně.

81 Tato kapitola je založena na výzkumu, jehož výsledky byly částečně publikovány v článcích Polčák, R., Říha, Z., Malinka, K. Právní aspekty interních směrnic - část I. Data Security Management, roč. XIX, číslo 2, str. 36–39 a Polčák, R., Říha, Z., Malinka, K. Právní aspekty interních instrukcí – část II. Data Security Management, roč. XIX., číslo 3, str. 36.

82 Viz Noeim, G. T.: Cybersecurity: Ideas Whose Time Has Not Come-and Shouldn't, I/S: A Journal for Law and Policy, roč. 8, číslo 2, str. 408.

83 Srov. Polčák, R.: Internet a proměny práva, Auditorium, Praha, 2012, str. *

Jestliže se tedy vysokou rychlostí řítí na veřejnou budovu auto naložené výbušninou, musí být v oprávněném instrumentáriu bezpečnostního personálu též technická a právní možnost střílet na jeho řidiče s cílem jej usmrtit. Může se pak jevit jako paradoxní, že oprávnění zabíjet má v tomto případě kdejaký policajt, zatímco dokonce ani sfinga Spravedlnosti (u nás zřejmě soudce Ústavního soudu) nemůže po roky trvajícím soudním řízení dospět k závěru, že je nutno nějakého člověka (libovolně provinilého) zbavit života. Tento paradox byl až tragicky evidentní například v případě Breivik. Dokud incident trval, měl právo tohoto šílence zastřelit každý, kdo by k tomu měl sebemenší příležitost - poté, co tragédie skončila tím, že se útočník vzdal, není v Evropě síly, která by ho dokázala legitimně zbavit života.

Právě uvedené nemá být rozhodně pochopeno jako argument ve prospěch razantnějších trestů (či dokonce Evropou snad již natrvalo zavrženého trestu smrti), ale pouze jako ilustrace závažnosti právních pravidel, jejichž cílem je nějaký aspekt bezpečnosti. Prostá nutnost mít k dispozici efektivní nástroj řešení bezpečnostní hrozby v tomto případě vede k tomu, co bychom mohli nazvat pochopitelně hypertrofovanou situační legitimitou.

Je v této situaci logické, že právní instrumenty, které bezpečnostním opatřením vytvářejí prostor k efektivnímu fungování, jsou kvůli svému destruktivnímu potenciálu pod permanentním drobnohledem různých forem demokratické kontroly výkonu veřejné moci[84]. K pochopitelné a priori nedůvěře k výkonné moci pak ještě přistupuje fakt, že jakákoli soudní či jiná kontrola užití těchto nástrojů může být až následná, v důsledku čehož je celá ničivá síla při svém užití prakticky výhradně v rukou exekutivy[85].

3.2 Individuální odpovědnost a ochrana prostředí

Když se cca před pěti lety začala v režii Národního bezpečnostního úřadu tvořit základní architektura zákona o kybernetické bezpečnosti, týkalo se jedno z nejdůležitějších rozhodnutí otázky, zda nebo do jaké míry by nová právní pravidla měla obsáhnout vedle správců informačních systémů a sítí

84 Viz Kelly, T. K.; Hunker, J. Cyber Policy: Institutional Struggle in a Transformed World, I/S: A Journal for Law and Policy, roč. 8, číslo 2, str. 210.

85 Viz Brenner, S.: Cyber-threats and the Limits of Bureaucratic Control, Minnesota Journal of Law, Science and Technology, roč. 14, č. 1, str. 137.

nebo poskytovatelů služeb informační společnosti též koncové uživatele. Bylo přitom samozřejmě jasné, že se koncových uživatelů může nová právní úprava v nějaké formě dotknout - podstatnou otázkou však bylo, zda se tak má stát formou přímé definice právních povinností respektive sankčního působení výkonné moci nebo jen zprostředkovaně v důsledku technických omezení a pravidel implementovaných jednotlivými správci příslušných informačních systémů a sítí.

V žádné civilizované zemi doposud v důsledku shora zmíněných rizik ohledně legitimity nepřistoupil právotvůrce k originárnímu založení aktivních povinností pro koncové uživatele. Přestože by se tedy možná nabízelo řešení kybernetické bezpečnosti ve smyslu zákonné objektivní odpovědnosti uživatele za bezpečnostní rizika, která generuje jeho systém, není k takovému řešení doposud politická vůle. Paralely s dopravními prostředky nebo domácími zvířaty v tomto směru jen těžko obstojí, neboť v případě informačních a komunikačních technologií jde o takovou míru technické složitosti a bezpečnostní zranitelnosti příslušných uživatelských systémů, která nemá obdobu v jiných oblastech běžného lidského života.

Právě zmíněný problém dobře ilustrují dávné případy odpovědnosti za škodu způsobenou v důsledku tzv. dialerů. Šlo o formy škodlivého kódu, který nepozorovaně přenastavil parametry vytáčeného internetového připojení a uživatel, namísto komunikace s providerem poskytujícím tuto službu zdarma nebo za běžnou cenu, připojoval se prostřednictvím některé z tzv. modrých linek za astronomické poplatky. V České republice byli uživatelé postižení tímto typem podvodného jednání do té míry smíření s osudem, že se proti němu nijak vehementně nebránili. V Německu naproti tomu řešil podobné případy dokonce Nejvyšší soud a dospěl k závěru, že nelze po běžném uživateli chtít takovou míru technologické bdělosti, která by jej před destruktivními následky působení dialeru ochránila. Výdělek modré linky byl tedy označen za nemravný a telekomunikačním společnostem, které v tomto případě fungovaly prostřednictvím účastnických smluv jako inkasní agentury, nezbylo, než účtovat za připojení jen běžné poplatky a na astronomické sazby zcela zapomenout (tam, kde skutečně došlo k výplatám provozovatelům modrých

linek ze strany telekomunikačních společností, musely být tyto platby prostě odepsány jako ztráta)[86].

Podobně benevolentní jsou k uživatelům též soudy (zde včetně českých) v případech sporů o náhrady škody způsobené krádeží identity u elektronického bankovnictví a elektronických platebních prostředků. Výjimkou tak u nás nejsou případy, kdy banka přinejmenším spoluodpovídá i za škody, které byly způsobeny v důsledku toho, že klient neměl svůj systém náležitě zabezpečen a útočník kvůli tomu získal možnosti disponovat s jeho bankovním účtem[87].

Jedinou formou přímé odpovědnosti za kybernetický útok, s níž se můžeme ve vyspělém světě setkat, jsou pasivní povinnosti, na nichž je postaven severoamerický model práva kybernetické bezpečnosti. Uživatel má v takto architektonicky pojatém řešení povinnost pasivně strpět zásah do svého soukromí, přičemž systém právních nástrojů je nastaven tak, aby bylo možno co nejlépe odhalit a následně usvědčit útočníka. Dokonce ani v prostředí, které je v porovnání s Evropou mnohem méně citlivé na otázku ochrany soukromí, však tento model doposud nezaznamenal politický úspěch a přes poslední vývoj je vzhledem k jeho konečné implementaci spíše důvod k mírné skepsi[88].

Členské státy EU, z nichž jako první představila širokospektrální legislativu v oblasti kybernetické bezpečnosti Česká republika, se naproti tomu rozhodly postavit svá právní řešení na nedistributivním přístupu, tj. na ochraně prostředí. Evropská legislativa tedy nemíří na koncového uživatele a nezakládá mu žádné aktivní nebo pasivní povinnosti. Namísto toho cílí na správce vybraných informačních systémů a sítí a ukládá jim povinnosti k užívání bezpečnostních technologií, zavádění efektivních organizačních řešení nebo hlášení výskytu bezpečnostních incidentů[89]. Analogicky s protipožární ochranou tedy v našem případě nejde v první řadě o nalezení a usvědčení pachatele ale o prevenci vzniku požárů a o jejich co nejefektivnější uhašení.

---

86 Viz Polčák, R.: Nedovolené přesměrování při připojení k internetu v rozhodnutí Spolkového soudního dvora, Jurisprudence, roč. XIV, číslo 3, str. 64.

87 Srov. např. rozhodnutí Nejvyššího soudu č. j. 29 Cdo 1180/2008, publ. prostř. www.nssoud.cz.

88 Viz Kesan, J. P.; Hayes, C. M.: Creating a ‚Circle of Trust' to Further Digital Privacy and Cybersecurity Goals, Illinois Public Law Research Paper No. 13-03, vyjde v Michigan State Law Review.

89 Viz návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM/2013/048 final - 2013/0027 (COD)*

Právě uvedené samozřejmě neznamená, že by ve členských státech EU nebylo možno stíhat pachatele počítačových útoků. Trestní agenda je ale v tomto případě hmotně, procesně i institucionálně oddělena od agendy kybernetické bezpečnosti. Specifická zákonná úprava kybernetické bezpečnosti se problematice vyšetřování a stíhání počítačových útoků věnuje až na výjimky pouze ve formě možností spolupráce orgánů veřejné moci odpovědných za správu národního systému kybernetické bezpečnosti a orgánů činných v trestním řízení. Ze specifických pravidel na úseku kybernetické bezpečnosti lze tedy v oblasti trestního postihu kybernetických bezpečnostních incidentů využít zejména povinností veřejnoprávních dohledových center předávat údaje o řešení kybernetických bezpečnostních incidentů pro potřeby přípravného nebo soudního řízení trestního.

3.3 Postih nezodpovědného uživatele

Odpovědnost za nedbalostní trestné činy nebo povinnosti nahradit škodu způsobenou nedbalostními civilními delikty představují z možností individuální odpovědnosti za kybernetické bezpečnostní incidenty pro právní praxi zřejmě nejaktuálnější výzvu. Teoreticky snadněji je sice v právní rovině řešitelná odpovědnost za úmyslné zavinění těchto incidentů, tj. v případě počítačových útoků odpovědnost samotných pachatelů. Vzhledem k velmi obtížné technické prokazatelnosti původcovství počítačových útoků a ke skutečnosti, že zdroj útoku bývá obvykle v zahraničí, jsou však reálné možnosti postihu z titulu úmyslné účasti na protiprávním jednání spíše hypotetické[90].

Přestože, jak uvedeno shora, nepřinesly nové předpisy v oblasti kybernetické bezpečnosti vzhledem k založení povinností koncových uživatelů žádné podstatné změny, lze v těchto případech postupovat dle standardních pravidel trestní či civilní deliktní odpovědnosti[91]. Předně je možno stavět na obecném civilistickém předpokladu, že každý odpovídá za škodu, kterou způsobí zaviněným protiprávním jednáním upravenou § 2910 a násl. občanského zákoníku. Za zavinění je přitom možno považovat i nevědomou nedbalost,

90 Srov. Završnik, A.: Towards an Overregulated Cyberspace: A Criminal Law Perspective, Masaryk University Journal of Law and Technology, roč. 4, číslo 2, str. 173.

91 Viz Hylton, K. N.: Property Rules, Liability Rules, and Immunity: An Application to Cyberspace, Boston University Law Review, roč. 87, číslo 1, str. 1 a násl.

tj. situaci, kdy je škoda způsobena uživatelem, který škodit nechce a dokonce ani neví, že jeho jednání či opomenutí může vést ke škodlivému následku - o tom, že ke škodě v důsledku takového jednání či opomenutí dojít může, však vědět má a může. V trestním právu pak, mimo jiné i vzhledem k principu ultimae rationis ve smyslu ust. § 12 odst. 2 trestního zákoníku, dle něhož tento typ sankce může stíhat jen ty nejzávažnější formy společensky nebezpečného jednání, jde především o skutkovou podstatu trestného činu obecného ohrožení z nedbalosti dle § 273 trestního zákoníku.

Právě základní předpoklad nevědomé nedbalosti, tj. že škůdce o možnosti způsobit škodu vědět má a může vyjádřená v § 2911 občanského zákoníku formulí „nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale," je klíčem k judikatornímu řešení otázky odpovědnosti uživatele v konkrétních případech kybernetických bezpečnostních incidentů. Pokud je totiž možno prokázat, že uživatel o určitém bezpečnostním riziku v daných okolnostech vědět měl a mohl, a škoda nastala v důsledku toho, že tuto skutečnost nijak neřešil, můžeme hovořit o založení povinnosti takto vzniklou škodu nahradit. Uživatel, který vědět má a může o tom, jak svůj systém zabezpečit a umožní jeho zneužití útočníkem (např. v typickém případě útoku typu DDoS), tedy bude povinen nahradit škodu, kterou tím způsobí.

Problémem takové právní kvalifikace přitom není absence konkrétního zákonného důvodu ale spíše otázka skutečné povinnosti uživatele vědět o zranitelnosti systému nebo o skutečnosti, že vůbec resp. jak je třeba systém průběžně záplatovat. Dalším praktickým (pragmatickým) problémem skutečného uplatnění tohoto typu odpovědnosti pak je kalkulace skutečné škody - uživatel totiž v tomto případě nemůže z podstaty věci odpovídat solidárně za celkovou škodu způsobenou útokem ale pouze za tu její část, která odpovídá míře jeho vlastního zavinění (v tomto případě jde o důvody hodné zvláštního zřetele ve smyslu § 2915 odst. 2 občanského zákoníku). V případě, kdy je útok veden velkým nebo dokonce neznámým počtem systémů, tedy může být žalobce ohledně konkrétní výše škody v důkazně problematické situaci.

Míra škodlivosti při zneužití uživatelského systému ke kybernetickému útoku je společně s prokazatelností toho, že dotyčný o bezpečnostním riziku a jeho

řešení vědět měl a mohl, logicky též překážkou uplatnění trestního postihu. Podobně jako v případě soukromoprávní povinnosti škodu nahradit zde není problém s tím, že by na příslušné situace nebylo objektivně možno aplikovat obecnou skutkovou podstatu trestného činu - hlavní otázka faktické použitelnosti tohoto typu odpovědnosti za nedbalostní účast na kybernetickém bezpečnostním incidentu totiž opět tkví v prokazatelnosti skutečného nedbalostního zavinění v kombinaci s rozsahem škodlivého následku. Na rozdíl od soukromého práva se však může trestní právo spolehnout na specifičtěji definované skutkové podstaty (vedle shora zmíněného nedbalostního obecného ohrožení to je zejména neoprávněné nakládání s osobními údaji ve smyslu ust. § 180 trestního zákoníku a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti ve smyslu ust. § 232 trestního zákoníku).

Typické případy, v nichž by připadala v úvahu (spolu)odpovědnost běžného uživatele za kybernetický bezpečnostní incident resp. za jeho následky, zahrnují např. vadnou manipulaci s heslem nebo různé formy nezodpovědného jednání (např. otevírání neznámých příloh v e-mailu nebo navštěvování nedůvěryhodných webů). Otázka skutečné povinnosti uživatele vědět o bezpečnostním riziku je v takových případech vždy závislá na okolnostech konkrétního případu, takže nelze dopředu určit, zda nebo v jaké míře lze uvažovat o právně relevantní nedbalosti. Záležet bude na pozici uživatele (tj. zda jde o soukromě jednající osobu, zaměstnance, úřední osobu apod.), jeho skutečné či povinné kvalifikaci, míře jeho předchozího proškolení apod. Z téhož důvodu není zřejmě ani účelné uvažovat nyní o specifičtější zákonné úpravě - jako vhodnější řešení jeví se spíše ad hoc aplikace shora zmíněných obecných odpovědnostních institutů a vzhledem k relativní vzácnosti případů, které si mohou najít cestu k soudu, není důvod se domnívat, že by nutnost důkladnějšího hodnocení skutkového stavu měla naše soudy jakkoli obtěžovat.

Velmi zajímavou možnost řešení individuální odpovědnosti uživatele přinesl doposud výjimečný případ, který řešily americké soudy. Šlo v něm, stručně řečeno, o infekci využívající bezpečnostní díru v systémech společnosti Microsoft, která umožňovala skryté využití napadených systémů jako součástí botnetu pro útoky typu DDoS. Spol. Microsoft se odhodlala k právně

originálnímu řešení, když zažalovala organizátory botnetu a v návrhu rozhodnutí též de facto navrhla postihnout i uživatele, kteří své systémy nezabezpečili záplatou[92].

Plán založit nepřímou odpovědnost koncových uživatelů jeví se být sice ve světle shora uvedených argumentů jako prostá marnost. V tomto případě se však spol. Microsoft podařilo velmi inovativním způsobem vyřešit rovnováhu mezi deliktem a jeho odpovědnostním důsledkem. Žalobní petit totiž nezněl na náhradu škody nebo jiné plnění, ale „pouze" na povinnost uživatele strpět dálkový zásah do svého systému, kterým Microsoft přesměruje za účelem vyšetření celého incidentu případný útok na své vlastní servery. Tento nárok byl díky tomu shledán proporcionálním k deliktu a následně přiznán. Microsoft tedy mohl nepozorovaně zasáhnout do infikovaných systémů a díky přesměrování jejich komunikace nejen zabránit škodám, které by botnet mohl způsobit, ale též získat cenná data k vyšetření celého incidentu.

Tento případ není pro českou právní praxi inspirativní do té míry, že by bylo snad možno uvažovat o podobném řešení v našich podmínkách. Naše procesní právo totiž nedovoluje žalovat na základě identifikačního znaku, nelze-li podle něj přímo v řízení ztotožnit konkrétní subjekt. I pro naše právní prostředí je však zajímavá úvaha soudu ohledně toho, že i běžný uživatel má určitou míru povinnosti vědět o potřebě zabezpečení svého vlastního systému a že tuto povinnost lze uvést do souvislosti s adekvátním typem odpovědnostního následku, tj. nikoli např. hradit škodu ale „pouze" strpět dálkový zásah do svého systému.

3.4 Postih příliš aktivního operátora

Jako naprostý paradox může se jevit skutečnost, že nejčastějším praktickým právním problémem kybernetické bezpečnosti týkajícím se individuální odpovědnosti je otázka možností postihu za různé typy činností souhrnně označovaných jako aktivní ochrana[93]. Individuální odpovědnost samotného

92 Viz Rozhodnutí rozhodnutí okresního soudu pro Western District of Notrh Carolina, Charlotte Division č. j. 3:13-CV-00319-GCM, dostupné na serveru botnetlegalnotice.com

93 Srov. Kesan, J. P.; Hayes, C. M.: Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, Harvard Journal of Law and Technology, roč. 25, číslo 2, str. 429.

škůdce je totiž problematická z důvodu složité důkazní situace v kombinaci s často přeshraničním charakterem počítačových útoků a odpovědnost uživatele je, jak uvedeno shora, obtížně dosažitelná především kvůli problematické argumentaci, že o riziku a jeho pokrytí vědět mohl a měl. Naproti tomu operátor, který proti kybernetickému bezpečnostnímu incidentu aktivně zasahuje, se neskrývá (resp. neměl by se skrývat) a vzhledem k tomu, že jde o profesionála, dobře ví, co dělá (resp. vědět to rozhodně má a může). Fenomén kybernetické bezpečnosti s sebou tedy mimo jiné přinesl do práva též potřebu určit hranice toho, co si lze při obraně před kybernetickými bezpečnostními incidenty dovolit.

V závislosti na typu techniky užité k ochraně systémů nebo sítí před kybernetickými bezpečnostními incidenty můžeme v souvislosti s možnou individuální odpovědností v první řadě hovořit o preventivních nástrojích. Potenciálně problematické jsou v tomto směru nejrůznější techniky souhrnně označované jako penetrační testování a nástroje, v důsledku jejichž užití dochází k monitorování soukromých aktivit uživatelů[94].

Druhou skupinou právně problémových forem ochrany systémů a sítí před kybernetickými bezpečnostními incidenty jsou různé techniky tzv. aktivní obrany. O základní klasifikaci, která reflektuje technické i právní požadavky na jejich systematizaci, se pokouší následující tzv. Dagstuhlská taxonomie[95]:

1. hack-back - tato technika spočívající v neautorizovaném průniku do systému útočníka, může být problémová z více důvodů. Především je obvykle třeba kromě útočníkova vlastního systému napadnout též řadu dalších systémů resp. služeb informační společnosti, které útočník ke své činnosti používá. Průnik do datových prostor může navíc kromě dat útočníka vystavit expozici též množství jiných typů dat, k nimž nemá obránce právo přistupovat.
2. steal-back - obvyklou formou aplikace této techniky je monitorování úložišť používaných útočníkem a průběžná reakce na zjištění zájmových dat (typicky např. formou zablokování uživatelského účtu v případě, kdy se v útočníkově dropzone objeví příslušné přihlašovací

94 Viz Cormack, A.: Can CSIRTs Lawfully Scan for Vulnerabilities? SCRIPTed, roč. 11, č. 3, str. 308.

95 Viz Freiling, F. C., Hornung. G. Polčák, R. (eds.); Forensic Computing – report from Dagstuhl Seminar 13482, Dagstuhl, Dagstuhl Publishing, 2014, str. 204.

údaje). Podobně jako v předchozím případě spočívá i zde problém vedle absentující autorizace především ve skutečnosti, že se obránce dostává i k datům, k nimž nemá práva přistupovat (může jít typicky o cizí přihlašovací údaje, osobní údaje apod.)

3. sinkholing - tato technika, kterou ve shora diskutovaném případě použila spol. Microsoft, vyžaduje především přístup a úpravu uživatelského systému, obojí bez vědomí uživatele resp. správce. Už sama skutečnost, že si spol. Microsoft vyžádala, byť nepřímo, k takovému jednání soudní puvoir, ukazuje na velkou pravděpodobnost absence implicitního zákonného dovolení
4. reverzní DoS - tato technika je především v případech decentralizované správy botnetu často jedinou možnosti efektivní obrany. Její užití však zpravidla znamená destruktivní protiútok na systémy, které jsou v botnetu zapojeny.
5. blacklisting a blokování - nejméně konfliktní metoda aktivní obrany může být právně problematická především v případech, kdy její užití objektivně naruší hospodářskou soutěž nebo se projeví jako obsahová cenzura. V těchto případech však je spíše důvod uvažovat o korporátní, nikoli individuální, odpovědnosti.

Každá ze shora uvedených technik je potenciálně právně problematická, přičemž v úvahu přichází v některých případech dokonce i trestní postih zejm. podle specifických skutkových podstat zavedených do českého práva na základě Úmluvy o počítačové kriminalitě - na rozdíl od shora zmíněného nedbalého jednání uživatele jde totiž v tomto případě o jednání úmyslné, byť nikoli s úmyslem přímo škodit. Vedle možnosti aplikace materiálního korektivu trestního práva hmotného ve smyslu ust. § 12 odst. 2 trestního zákoníku je vyloučení odpovědnosti jednotlivce za jejich užití především otázkou rozsahu institutů krajní nouze, nutné obrany nebo přípustného rizika (§ 28, § 29 a § 31 trestního zákoníku).

Zdá se, že situace ohledně odpovědnosti profesionála zabývajícího se aktivní ochranou informačního systému nebo sítě, je ve vztahu k možné jeho individuální odpovědnosti obdobná jako ve shora diskutovaném případě (ne) poučeného uživatele. Zatímco však je tato nejistota uživateli spíše ku prospěchu, vede u zájemců o aplikaci metod aktivní ochrany k často neadekvátní opatrnosti. Výjimkou nejsou případy, kdy si i velké korporace najímají

k aktivní ochraně svých systémů externí dodavatele (často fungující téměř podzemním způsobem) ze strachu, aby na ně nedopadl případný postih. Bezpečnostní experti pracující i pro všeobecně známé soukromoprávní korporace pak musí svého skutečného zaměstnavatele často tajit a stejně musí skrývat, nezřídka i před vlastní rodinou, předmět své pracovní činnosti.

Ve výsledku tak z této opatrnosti založené právní nejistotou plyne faktické potlačování rozvoje a užití nástrojů, které by mohly výrazně vylepšit celkovou bezpečnostní situaci naší informační společnosti. Zatímco jsme tedy shora konstatovali obecnou aktuální vhodnost aplikace obecných odpovědnostních institutů na jednání běžného uživatele, máme v případě technik aktivní ochrany spíše důvod považovat absenci konkrétnějších zákonných pravidel za naléhavou legislativní objednávku.

3.5 Interní instrukce jako bezpečnostní opatření

Základním kamenem českého práva kybernetické bezpečnosti jsou bezpečnostní opatření. Jedná se o obecné standardní požadavky, jejichž implementací mají povinné subjekty zajistit základní úroveň bezpečnosti vyžadovanou k ochraně národních zájmů na fungování informačních a komunikační infrastruktury[96]. Zákon a prováděcí vyhláška používají problémový přístup k definicím jednotlivých skladebných prvků bezpečnostních opatření, jejichž objektové shrnutí lze provést následovně[97]:

1. Technické prvky (specifický software a hardware vč. detekčních systémů, reportovacích nástrojů, autentizačních či kryptografických nástrojů, technika k zajištění fyzické bezpečnosti apod.)
2. Analytické prvky a dokumentace (typicky analýza informačních aktiv, topografie sítí, analýza rizik apod.)

96 Zákon je v § 4 odst. 1 vymezuje jako „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru".

97 Problémovou specifikaci obsahují ust. § 5 odst. 2 a 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Prováděcím předpisem je vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

3. Interní předpisy (organizační opatření, školící plány, krizové plány, interní instrukce pro vybrané skupiny zaměstnanců, interní pravidla pro nákup a outsourcing ICT apod.)
4. Lidské zdroje (specificky vyčleněný personál k zajištění realizace bezpečnostních opatření nebo personál zajišťující výjimečně ad hoc určité činnosti v oblasti kybernetické bezpečnosti)

Pokud bychom měli z výše uvedených vybrat nástroj, u něhož se nejvýrazněji projevuje shora zmíněný problém vzájemného porozumění dotčených vědních oborů, nepochybně jím budou interní předpisy. Informatik nebo manažer totiž má tendenci chápat interní bezpečnostní předpis jako komplexní návod na to, jak se má uživatel nebo správce příslušného informačního systému chovat, tj. jako kuchařku poskytující recept na bezpečné používání příslušné informační nebo komunikační technologie.

Takové pojetí interního předpisu se však s jeho právní náturou srovnává jen velmi těžko. Dále se pokusíme nejprve odpovědět na otázku, jaký je smysl a účel interního předpisu upravujícího v rámci soukromoprávní nebo veřejnoprávní korporace problematiku kybernetické bezpečnosti. V návaznosti na to se pak pokusíme o identifikaci a analýzu faktorů, které jsou z pohledu platného práva klíčové ve vztahu k právní existenci (platnosti) interních předpisů a k jejich konformitě s aktuálními zákonnými požadavky.

3.6 Nevhodný obsah interních bezpečnostních instrukcí

Předně je třeba konstatovat, že má-li něco formu interního předpisu, jedná se o jednostranný akt, jímž nadřízený zavazuje své podřízené k určitému typu chování. Interní předpis nemá sice vyložené vrchnostenský charakter[98], ale jeho závaznost je dána zákonným vztahem nadřízenosti resp. podřízenosti, v jehož rámci je zaměstnanec povinen plnit pracovní úkoly dle pokynů

98 Interní instrukce se na rozdíl od normativního nebo individuálního vrchnostenského aktu nemůže spoléhat na presumpci správnosti resp. presumpci platnosti – srov. Bělina, M. a kol. Pracovní právo. 5. dopl. a podstat. přeprac. vyd., Praha: C. H. Beck, 2012, str. 66.

zaměstnavatele. Interní předpis tedy nemá činit ni jiného, než neadresně[99] zakládat zaměstnancům specifické povinnosti přímo se týkající jejich pracovní náplně[100].

Z právě uvedeného předně plyne, že předmětem interní instrukce nemají být povinnosti, které zaměstnancům vyplývají v obecně závazných právních předpisů. Ustanovení typu „zaměstnanec je povinen dodržovat ustanovení zákona č. 101/2000 Sb." je tedy zčásti zbytečné a zčásti může být dokonce pro zaměstnavatele i právně rizikové. Zákonné právo je totiž plné relativně abstraktních ustanovení. Nejistoty ohledně interpretace nejasných pojmů typu „osobní údaj" se pak sice nelze dovolávat vůči státu, ale je-li text zákona tímto způsobem učiněn součástí interního předpisu, může zaměstnanec namítat tuto neurčitost v případě disciplinárního postihu.

K tomu pak především u odkazů na komplexní právní předpisy přistupuje i možnost, že zákon dává v určitých situacích právo výběru z více typů chování nebo zakládá nižší standard povinností, než které má zaměstnavatel zájem rigorózněji upravit interním předpisem. Je-li však zákon de facto učiněn součástí interního předpisu, dává to zaměstnanci důvod vymluvit se na neurčitost vnitřního předpisu, který tím pádem v různých svých částech stanoví tytéž povinnosti různým způsobem.

---

99 Neadresnost odlišuje interní instrukci od aktu řízení, jímž je uložena povinnost konkrétnímu pracovníkovi. Interní instrukce však musí být zaměřena tak, aby bylo možno vždy určit pracovníka, kterého zavazuje. Pokud z instrukce není jasné, koho má zavazovat, nezavazuje nikoho a z právního hlediska na ni můžeme hledět, jakoby nebyla – příkladem může být čl. 8 odst. 1 směrnice MU č. 6/2011 následujícího znění: „MU se snaží chránit práva a oprávněné zájmy všech uživatelů své sítě a v této souvislosti i chránit data a informace uložené na počítačích MU nebo přenášených sítí MU. MU však nemůže technicky zabezpečit úplné soukromí a bezpečnost dat uložených na počítačích nebo přenášených sítí. Vysoce citlivá data proto nemohou být na počítačích sítě uložena či sítí přenášena bez použití dodatečných prostředků jejich zabezpečení (minimálně na úrovni šifrování)." Vedle toho, že ustanovení nemá zčásti normativní povahu (jedná se o vysvětlení resp. snad o omluvu) a není jasné, komu z něj plynou nějaké povinnosti, objevuje se zde i zajímavý problém užití aletické modality „nemohou" namísto adekvátní modality „nesmí." Citlivá data (ať už to znamená cokoli) totiž v tomto případě samozřejmě mohou být uložena na počítačích MU – směrnice má ale zajistit, aby se tak nestalo tím, že deonticky zakáže jednání, které by k tomu mohlo vést.

100 Rozdíl mezi interní instrukcí a aktem řízení spočívá v tom, že zatímco interní instrukce je určena neurčitému okruhu pracovníků splňujících určitou podmínku (např. pracovníkům v určité funkci), je akt řízení adresován, tj. určen konkrétnímu člověku. K povaze interní instrukce viz např. Galvas, M. a kol. Pracovní právo. Brno: Masarykova univerzita, 2012, str. 50 nebo Vysokajová, M. Zákoník práce - komentář. Praha: Wolters Kluwer, 2012, str. 623.

Velmi problematické jsou též situace, kdy si zaměstnavatel při vydávání vnitřních předpisů formou odkazů na zákonnou úpravu usnadňuje situaci, resp. předpokládá, že jakékoli porušení citovaného zákona ze strany zaměstnance bude automaticky možno považovat za disciplinární delikt (s následnou možností uplatnění disciplinární sankce typu okamžitého zrušení pracovního poměru). V takovém případě při porušení zákonné povinnosti ze strany zaměstnance nelze automaticky hovořit o disciplinárním prohřešku – tím méně v typických případech, kdy jde o nedbalostní porušení komplikovaných technických pravidel, které nemají přímý vztah k vykonávané práci. Skutečnost, že takové porušení sama směrnice označí za obzvláště hrubé porušení pracovních povinností, na tom nic nemění.

Podobně, jako není vhodné do interních instrukcí přebírat zákonné povinnosti, nelze doporučit ani úpravu banalit. Typickým problémem jsou v tomto směru definice, jimiž často bezpečnostní předpisy začínají a které se týkají pojmů, jejichž význam je obsažen v běžném jazyce. Můžeme se tak v praxi setkat s definicemi pojmů, jako je mobilní telefon, počítač nebo počítačová síť'[101]. Problémem těchto definic často bývá i v jejich složitosti, přičemž čím větší je snaha o jejich přesnost, tím delší a méně srozumitelné bývají – autor snažící se definovat veškeré pojmy co nejpreciznějí se přitom často nevyhne užití neurčitých výrazů typu „zejména" nebo „především," které ve výsledku přinášejí totální relativizaci jejich obsahu[102].

101 Příkladně směrnice MU č. 6/2011 definuje počítač jako „jakékoliv technické zařízení disponující výpočetním výkonem připojitelné do počítačové sítě" a počítačovou síť jako „technické a programové prostředky používané k propojení počítačů." Dle této definice lze přitom za počítač považovat i běžnou tiskárnu a za počítačovou síť USB kabel, kterým se tiskárna připojuje k počítači (resp. k tomu, co by za počítač běžně označil rozumně uvažující pracovník bez technického vzdělání). Jediným štěstím v tomto směru je, že směrnice nedefinuje jinak mnohem neurčitější pojmy jako „technický prostředek" nebo „programový prostředek."

102 V mnoha směrech odstrašujícím didaktickým příkladem je definice studené omáčky obsažená ve vyhlášce č. 331/1997 Sb., kterou se provádí § 18 písm. a), d), h), i), j) a k) zákona č. 110/1997 Sb., o potravinách a tabákových výrobcích a o změně a doplnění některých souvisejících zákonů, pro koření, jedlou sůl, dehydratované výrobky a ochucovadla a hořčici, ve znění pozdějších předpisů, následovně: „[studenou omáčkou nebo dresingem se pro účely této vyhlášky rozumí] tekutý nebo emulzní výrobek používaný jako chuťová příloha k pokrmům a salátům, vyrobený zejména z jedlých olejů, zahušťovadel, stabilizátorů, emulgátorů, zeleniny, ovoce, koření a mléčných výrobků" – není třeba přílišné představivosti k tomu, aby čtenáři došlo, že dle této definice může být studenou omáčkou prakticky cokoli, co teče (a nemusí to být ani studené).

Namísto nekonečného definování běžných pojmů je třeba předně řešit otázku adresáta příslušného předpisu a založit text na takových výrazových prostředcích, které odpovídají jeho kvalifikaci resp. jeho pracovnímu zařazení. Typicky tedy lze od pracovníka, u jehož pozice je vyžadována znalost práce s PC, očekávat, že bude mít vcelku konkrétní představu ohledně toho, jak vypadá počítač nebo co to je přístupové heslo. Případné pochybnosti zaměstnavatele ohledně toho, zda zaměstnanci příslušné pojmy použité v interních předpisech skutečně ovládají, je pak lépe řešit formou didaktických nástrojů (viz dále).

Právě uvedené se netýká pouze definic, ale též banálních pracovních povinností. Není tedy nutno do interních předpisů týkajících se kybernetické bezpečnosti zahrnovat samozřejmé zásady bezpečné práce s počítačem, jejichž znalost lze na příslušném typu pracovního místa předpokládat. Příkladem může být obligátní psaní přístupových hesel na žluté lístečky a jejich lepení na monitory či klávesnice. Pokud už má z nějakého důvodu zaměstnavatel obavu ohledně základní intelektuální bezpečnostní výbavy svých zaměstnanců, je to podobně jako v případě banálních definic vhodnější řešit formou jejich cíleného vzdělávání (nikoli formou zavádění specifických pracovních povinností interními předpisy).

Vedle shora zmíněných zákonných povinností a banalit nehodí se do interních instrukcí ani povinnosti, jejichž plnění je z hlediska účelu nesmyslné nebo z hlediska reálných možností zaměstnance nemožné. Otázka smysluplnosti různých typů povinností k zajištění kybernetické bezpečnosti v rámci organizací je přitom vysoce problematická – chybí totiž relevantní výzkum, jehož předmětem by bylo hodnocení vlivu běžně užívaných povinností na reálnou bezpečnost příslušných systémů.

Obecně však lze konstatovat, že interním předpisem založená povinnost, jejíž faktický efekt na míru bezpečnosti je žádný nebo vysoce diskutabilní, nemůže zavazovat. Důvodem je omezení věcného rozsahu povinností ukládaných interními předpisy na takové, které mají vztah k vykonávané práci. Pokud tedy zaměstnavatel upraví povinnost, jejíž reálný efekt se práce vykonávané zaměstnancem nedotýká (v tomto případě by šlo o povinnosti s nulovým dopadem na zabezpečení příslušné informační infrastruktury), nemusí se zaměstnanec takovým předpisem cítit vázán.

Podobný důsledek, tj. absenci závaznosti, mají požadavky interních předpisů, které vzhledem k běžnému fungování zaměstnance na určité pracovní pozici nejsou reálně proveditelné. Je-li tedy zaměstnanci pracujícímu na pozici referenta uložen zákaz kamkoli si poznačit své přístupové heslo současně s povinností přístupové heslo znát, měnit jej každý týden a stanovit jej tak, aby obsahovalo minimálně 15 znaků, lze jen těžko takovou povinnost v případě jejího nesplnění disciplinárně sankcionovat.

3.7 Zákonná konformita interní instrukce

Předmětem toho krátkého pojednání samozřejmě nemůže být pouze výklad ohledně toho, co vše nemá být součástí interního předpisu týkajícího se kybernetické bezpečnosti, ale je třeba zaměřit se s minimálně stejnou pozorností i na otázku, co naopak v takové interní instrukci být má. V tomto směru je problémem především skutečnost, že zákonné právo je v otázkách konkrétních (individuálních) povinností při zabezpečení informačních systémů a sítí značně obecné. Tato skutečnost přitom není sama o sobě na závadu – jednou ze základních myšlenek regulatorní techniky zákona o kybernetické bezpečnosti je totiž takové založení povinností, které umožní na úrovni povinných subjektů[103] zvolit konkrétní metodu resp. postup, který bude co nejlépe odpovídat typu, velikosti či struktuře příslušných systémů a sítí. Zákon totiž správně předpokládá, že právotvůrce nemá dostatek konkrétních znalostí k tomu, aby mohl upravit povinnosti jednotlivým profesím, respektive že není možno v tomto směru vytvořit jeden nebo několik standardních řešení typu one-size-fits-all[104].

103 Povinnými subjekty jsou v případě české právní úpravy vždy správci příslušných systémů nebo sítí – nikdy nejde o konkrétní fyzické osoby. Správcem je pro potřeby zákona č. 181/2014 Sb. analogicky s definicí obsaženou v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, subjekt, který určuje účel provozu příslušného informačního systému nebo sítě – povinnosti pak zákon stanoví právě jemu. K tomuto přístupu viz např. Berejka, M. A Case for Government Promoted Multi-Stakeholderism, Journal on Telecommunications and High-Tech Law, roč. 10, str. 9.

104 Důvodová zpráva k zákonu o kybernetické bezpečnosti k tomu v části 1.5 uvádí: „Konkrétní organizační a technické postupy včetně např. řízení dodavatelů, školení zaměstnanců, interních kontrol apod. tedy ponechává navrhovaná právní úprava plně v diskreci povinných osob. Tím je zajištěno, že výsledné zabezpečení informačních a komunikačních systémů bude ve svém souhrnu spolehlivě funkční, přičemž individualita jednotlivých partikulárních bezpečnostních řešení umožní efektivní využití příslušných zdrojů."

Tato volnost, jakkoli logická a systematicky vhodná, však povinným subjektům přináší též nejistotu ohledně toho, co konkrétně a jak mají v interních předpisech upravit. Prvním problém představuje otázka, co a jak do interního předpisu napsat, aby předpis plnil požadavky zákona o kybernetické bezpečnosti a prováděcí vyhlášky Národního bezpečnostního úřadu. Interní předpis či předpisy totiž nemají jen význam pro faktickou realizaci bezpečnostních opatření na jednotlivých pracovištích se zvýšenou informačně-bezpečnostní expozicí, ale představují, jak uvedeno shora, nedílnou součást bezpečnostních opatření, jejich nasazení je pro povinné subjekty mandatorní. Interní předpisy tedy musejí upravovat problémové okruhy, která zákon a prováděcí vyhláška předepisují.

Vzhledem k tomu, že zákon vstoupil v účinnost teprve s počátkem roku 2015 a kontrolní činnosti ohledně souladu bezpečnostních opatření se zákonnými požadavky začnou vzhledem k přechodným obdobím probíhat nejdříve za rok, nelze se v otázce zákonné konformity spoléhat na aktuální kontrolní či rozhodovací praxi Národního bezpečnostního úřadu nebo na judikaturu správních soudů. Daleko od pravdy nebude zřejmě tvrzení, že ani sám Národní bezpečnostní úřad nemá v tuto chvíli konkrétní představu ohledně toho, jak by měly interní předpisy plnící požadavky zákona o kybernetické bezpečnosti vlastně vypadat.

Negativní aspekty relativní právní nejistoty ohledně konkrétního znění interních předpisů může poněkud mírnit očekávání v tom směru, že v otázce jejich zákonné konformity bude zřejmě Národního bezpečnostní úřad praktikovat při své kontrolní a sankční činnosti minimálně zpočátku spíše shovívavý přístup. Pomoci by v tomto směru mohly též oborové iniciativy, které sdružují povinné subjekty a mohou formou agregace odborných kapacit s přijatelnými náklady tvořit standardní formy interních instrukcí vhodných pro typické konkrétní aplikace například v energetice, telekomunikacích nebo v činnosti místních utilit[105].

[105] Typickým příkladem je aktuální činnost Technologické platformy energetická bezpečnost (TPEB) sdružujících energetické společnosti a společnosti provozující místní síťové utility, která by měla vést k založení a rozvoji příslušných oborových standardů a best practices.

Typové dokumenty cílené na určité aplikace mohou plnit roli vzorů, přičemž jejich oborové zaměření může zajistit jejich přiblížení reálné praxi – povinné subjekty tedy budou moci tyto oborově specifické vzory vzájemně přebírat s nutností pouze minimálních úprav týkajících se partikulárních technických aspektů. Důležité z hlediska efektivity je, že zákonná konformita a disciplinární závaznost (viz dále) bude vyřešena na úrovni vzoru, jehož úpravy pak už nemusí provádět právní expert, ale postačí k tomu technik resp. bezpečnostní specialista se znalostí místní infrastruktury. Korporátní právník pak nemusí mít specifické znalosti v oboru kybernetické bezpečnosti, ale může pouze dohlédnout na to, aby partikulární úpravy vzoru nenarušily jeho základní obsahové parametry. Velmi vhodné v tomto směru rovněž je, pokud k takové oborové koordinaci dojde za současné komunikace s Národním bezpečnostním úřadem – i z jeho pohledu totiž může standardizace interních instrukcí u různých typů povinných subjektů usnadnit následnou kontrolní činnost[106].

3.8 Srozumitelnost interní instrukce a bezpečnost z podstaty

Na rozdíl od zákona se interní instrukce nemohou spoléhat na luxus principu ignoratia legis neminem excusat, jehož komponentou je i zásadní nemožnost vymlouvat se na (často reálně existující) složitost či nesrozumitelnost psaného práva. Pokud tedy má zaměstnavatel zájem založit zaměstnanci specifickou povinnost jinak než přímým pokynem, tj. adresným imperativem, musí to učinit tak, aby tomu zaměstnanec byl za daných okolností schopen porozumět. Reálná srozumitelnost interní instrukce je tedy nutným předpokladem její závaznosti[107].

106 Nelze samozřejmě uvažovat o tom, že bude soukromě vytvořený standard uznán resp. vynucován veřejnou mocí. Je ale v tomto směru otázkou kontrolní diskrece Národního bezpečnostního úřadu, pokud v případech, kdy bude aplikováno řešení tvořící neformální oborový standard, bude kontrola prováděna nikoli ve vztahu k samotnému standardu, ale pouze k jeho konkrétní implementaci.

107 V jednom z mediálně vděčných případů se k této otázce vyslovil i Nejvyšší soud, když se zabýval otázkou srozumitelnosti ústně sdělené interní instrukce týkající se bezpečnosti práce. V rozhodnutí Sp. zn. 21 Cdo 2141/2011 se píše: „Korektním pokynem k zajištění bezpečnosti a ochrany zdraví při práci proto mohl být (byl-li učiněn) i pokyn předáka P. (doslovně – ‚kurva, nelezte tam na ty světlíky, můžete sletět'), neboť tím stanoví pro podřízené závazný způsob chování a vysvětluje důvod svého pokynu."

V případě interních instrukcí v oboru kybernetické bezpečnosti představuje problém především určení míry odborného předporozumění[108], kterou lze od zaměstnance na určité pozici očekávat (to je ostatně i shora diskutovaná otázka banálních povinností, jež lze z interní instrukce vzhledem k očekávané kvalifikaci zaměstnance zcela vyloučit). Z toho plyne i nutnost diverzifikace obsahu interních bezpečnostních instrukcí v návaznosti na jejich adresáty. Je tedy třeba psát jinak interní instrukce pro správce sítě, bezpečnostního technika nebo pro office managera – to nikoli jen z toho důvodu, že se jejich povinnosti při zabezpečení příslušné informační a komunikační infrastruktury mohou (musí) lišit, ale i proto, že u nich lze očekávat jinou míru schopností rozumět a dostát specifickým technickým požadavkům.

Největší pozornost je třeba v tomto směru věnovat zaměstnancům, jejichž předmětem činnosti není přímo obsluha informačních a komunikačních technologií, tj. prostým uživatelům. Těm je totiž nutno sdělit bezpečnostní požadavky tak, aby je byli schopni pochopit a dodržovat bez nutnosti studia nad rámec kvalifikace vyžadované pro jejich pracovní pozici. Není vhodné stanovit předpisem například povinnost mít jako součást hesla „speciální znaky ASCII" bez vysvětlení, co to znamená ASCII, resp. o jaké znaky konkrétně jde. Ze stejného důvodu nelze bez dalšího zavést zaměstnancům typu uživatel například povinnost používat pro veškerou komunikaci šifrování RSA se 128 bitovým klíčem.

Z výše uvedeného nepřímo vyplývá, že problém korporátního řešení kybernetické bezpečnosti spočívá mimo jiné i v tom, že ke splnění zákonných požadavků či k zajištění obstojné bezpečnostní úrovně příslušné informační a komunikační infrastruktury je často nutno požadovat od běžných uživatelů takovou technickou orientaci, jíž vzhledem ke kvalifikaci potřebné k výkonu svých profesí nejsou schopni ani povinni. Rovněž lze ze shora uvedených poznatků uzavřít v tom smyslu, že tento problém není řešitelný formou interních instrukcí, které by tyto zaměstnance ke specifickým technickým povinnostem prostě zavázaly, ať jim jsou schopni porozumět či nikoli.

Řešením může být předně důkladná analýza skutečných bezpečnostních potřeb vzhledem k uživatelům a vyloučení těch povinností, které jsou

108 K pojmu viz práci Esser, J. Vorverständnis und Methodenwahl in der Rechtsfindung: Rationalitatsgrundlagen richterlicher Entscheidungspraxis, Frankfurt: S. Fisher, 1972.

z hlediska faktických a zákonných požadavků zbytné. U nezbytně nutných bezpečnostních opatření pak je na místě ptát se, zda není možno zajistit je jinak než založením povinností příslušným uživatelům, tj. především aplikací technických řešení resp. nástrojů, které realizaci bezpečnostních opatření dokáží zajistit bez ohledu na uživatelskou vůli. Nabízí se v tomto případě srovnání s fyzickou bezpečností, přičemž je namísto vydávání instrukce „každý je povinen za sebou zavírat dveře" zpravidla právně i technicky jednodušší pořídit na dveře zařízení, které je po průchodu člověka prostě zavře samo[109].

Až v případě nezbytných a nezastupitelných specifických povinností uživatelů pak je vhodné přistoupit k jejich úpravě formou vnitřního předpisu – tomu však musí předcházet náležité proškolení uživatelů tak, aby obsah předpisu byli schopni pochopit a jeho požadavkům mohli technicky dostát. Jakýkoli jiný postup vedle své problematické efektivity generuje též právní riziko spočívající v nejistotě ohledně právní závaznosti povinností založených interní instrukcí. Pokud tedy zaměstnavatel nebude respektovat výše uvedená doporučení, vystavuje se riziku nemožnosti uplatnit disciplinární sankci nebo vymáhat náhradu vůči zaměstnancům, kteří mu jednáním v rozporu s interními instrukcemi přivodí škodu.

3.9 Interní instrukce a problém soukromí na pracovišti

Výše jsme konstatovali, že smyslem interních instrukcí je zakládat originální povinnosti. Ty tvoří součást obsahu právního vztahu založeného mezi zaměstnancem a zaměstnavatelem. Standardní právnická typologie přitom kromě typu facere (konat) ještě rozeznává povinnosti typu dare (něco dát – ty jsou v pracovněprávních vztazích až na výjimky na straně zaměstnavatele), omittere (nekonat – tj. nedělat to, co by jinak dělat šlo) a konečně pati, tj. strpět nějaký zásah do subjektivních práv, proti kterému by jinak bylo možno se bránit.

109 V obvodu Městského státního zastupitelství Brno byla v přípravném řízením trestním řešena zajímavá otázka míry odpovědnosti uživatele, který protiprávně manipuloval s daty zaměstnavatele. Problém na straně zaměstnavatele však spočíval v tom, že, ačkoli velmi snadno mohl, neomezil práva v přístupu zaměstnance k vlastnímu systému. Zaměstnavatel tedy v tomto případě nevyužil možnosti zamezit zaměstnanci aleticky v přístupu k údajům, s nimiž neměl noc do činění, na úrovni přístupových práv k systému a namísto toho spoléhal pouze na deotické imperativy platné právní úpravy a vnitřních předpisů. Případ však neskončil obžalobou, pročež nám vzhledem k právním důsledkům liknavosti zaměstnavatele nepřináší žádné konkrétní závěry.

Posledně jmenovaný typ je pro interní instrukce v oblasti kybernetické bezpečnosti srovnatelně důležitý, jako povinnosti typu facere diskutované v předchozích kapitolách. Formou interní instrukce je totiž možno založit zaměstnancům povinnost strpět zásah do svých osobnostních práv, z nichž nejvíce exponované je v tomto případě právo na ochranu soukromí.

Právních otázek, které v souvislosti s nutností omezit soukromí zaměstnance na pracovišti resp. soukromí zaměstnance při práci, je celá řada a často nemají jednoznačné řešení[110]. Nejde zde v první řadě o jinak problematickou souvislost mezi ochranou soukromí a ochranou osobních údajů, ale spíše o otázku formy a především rozsahu takového omezení[111]. Podobně jako u povinností typu facere je tedy nutno řešit způsob, kterým zaměstnanci sdělit, že určité aspekty jeho pracovní činnosti mohou být specificky monitorovány resp. způsob, kterým monitorování provádět i bez toho, aby o tom zaměstnanec věděl. Srovnatelně problematické pak je určení míry toho, jak daleko může zaměstnavatel zajít při monitorování aktivit zaměstnanců pro potřeby zajištění bezpečnosti své informační a komunikační infrastruktury, resp. při plnění zákonných povinností.

V české literatuře se v tom směru v minulosti objevilo hned několik krátkých statí hájících extrémní pozice – je to dáno skutečností, že původcem těchto textů bývají u nás zpravidla advokáti hájící zájmy jedné ze stran typických pracovněprávních sporů[112]. V těchto sporech jde vesměs o to, že zaměstnavatel nasadí monitorovací nástroje na aktivity zaměstnance prováděné prostřednictvím pracovních informačních a komunikačních technologií (osobních počítačů, mobilních telefonů apod.) a jejich prostřednictvím získá důkazy například o tom, že zaměstnanec v pracovní době namísto plnění pracovních úkolů lelkuje, řeší si osobní záležitosti nebo dokonce pomáhá konkurenci. Následný vyhazov pak se stává předmětem sporu o zákonnost

110 Srov. např. Levin, A. Is There a Global Approach to Workplace Privacy? in Zureik, E., Stalker, L. H., Smith, E., Lyon, D., Chan, Y. E. Surveillance, Privacy and the Globalization of Personal Information, Montreal: cGill-Queen's University Press, 2010, str. 328 a násl.

111 Srov. např. Taylor, L. M. D. The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era, Minnesota Journal of Law, Science & Technology, roč. 15, číslo 2, str. 1015 a násl.

112 Světlou výjimkou je např. text Aujezdský, J. Skutečně může zaměstnavatel číst Vaší poštu?, server itpravo.cz, 20. 1. 2004, cit. 1. 2. 2015.

a klíčovou roli hraje právě otázka způsobu, jímž byly klíčové důkazy svědčící v zaměstnancův neprospěch získány[113].

Feudalistická extrémní pozice je v tomto směru založena především na argumentech vlastnickým právem a stojí na předpokladu, že zaměstnavatel jako (zpravidla) vlastník příslušné informační a komunikační infrastruktury má ultimátní právo rozhodovat, jak bude tato infrastruktura fungovat. Jestliže se tedy rozhodne pro nasazení logovacích nebo monitorovacích nástrojů, má k tomu z titulu svého vlastnictví plné právo a zaměstnanec s tím musí být srozuměn (to dokonce i v případě, že jej o tom zaměstnavatel explicitně neinformuje). K tomu pak může ještě přistoupit argument „vlastnictvím času," který si zaměstnavatel od zaměstnance formou pracovněprávního vztahu vlastně „kupuje[114]."

Především v případech použití pracovních prostředků pro soukromé účely objevuje se na straně žalujícího zaměstnance[115] anarchistická pozice postavená především na argumentu oprávněného očekávání zaměstnance v tom směru, že kontrola ze strany zaměstnavatele dá se předpokládat pouze ve vztahu k plnění pracovních povinností. Pokud však zaměstnavatel zaměstnanci žádné konkrétní povinnosti neukládal nebo zaměstnanec neměl jiné indicie toho, že by s jeho pracovním výkonem neměl být zaměstnavatel spokojen, neměl zaměstnavatel právo nasadit na aktivity zaměstnance sledovací prostředky. K tomu pak ještě může přistoupit argument ohledně toho, že použití informační a komunikační infrastruktury zaměstnavatele k zábavě nebo jiným soukromým aktivitám zaměstnance nevede zpravidla k jejich amortizaci a že skutečnost, že zaměstnanec v práci zahálí, je problémem zaměstnavatele neschopného přidělit mu práci.

Adekvátní řešení obecného problému ochrany soukromí na pracovišti neleží v tomto případě na nějaké zlaté střední cestě mezi zmíněnými extrémy, ale je otázkou vzájemné proporcionality dotčených práv zaměstnavatele (zde

113 Jedním z nejdůležitějších případů byl v tomto směru spor Coplandová proti Spojenému království, který ve prospěch stěžovatelky rozhodl Evropský soud pro lidská práva pod č. j. 62617/00. Plný text rozhodnutí je on-line ke stažení na adrese hudoc.echr.coe.int.

114 Srov. Wheelwright, K. Monitoring Employees' Email and Internet Use at Work - Balancing the Interests of Employers and Employees, Journal of Law, Information and Science, roč. 13, číslo 1, str. 70.

115 V těchto případech totiž obvykle pracovník žaluje svého (někdejšího) zaměstnavatele pro nezákonnost výpovědi – to byl i případ op. cit. v pozn. 25.

zejména práva vlastnického) a zaměstnance (zde zejména práva na ochranu soukromí) v konkrétním případě. Ta nemá obecný charakter, neboť vždy závisí na určujících okolnostech konkrétní pracovní situace a je dána faktory jako typ práce, charakter pracoviště nebo možnost existence konkrétního podezření ve vztahu k aktivitám zaměstnance[116]. Roli mohou hrát i na první pohled obskurní hlediska, jako jsou třeba věk nebo pohlaví zaměstnance, roční období apod.

Obecně přitom platí, že i na pracovišti má zaměstnanec soukromí a že součástí jeho soukromé sféry mohou být i prvky informační a komunikační infrastruktury zaměstnavatele. Typicky jde o osobně přidělovaná mobilní komunikační zařízení, notebooky nebo o nesdílené stolní počítače. Vzhledem k nim pak má zaměstnanec oprávněné očekávání ochrany soukromí a zaměstnavatel tedy nemůže do jejich informační integrity libovolně zasahovat[117].

Tam, kde je součástí bezpečnostního opatření monitorovací nebo obdobná komponenta, je předně třeba řešit otázku, zda má zaměstnanec v rozsahu jejího fungování o jejím nasazení vědět. Bez vědomí zaměstnance ji lze použít v následujících případech[118]:

- Monitorování se týká pouze kvantitativních parametrů týkajících se fungování příslušného systému nebo sítě,
- monitorování odpovídá bezpečnostní expozici příslušného systému nebo sítě (z čehož plyne skutečnost, že zaměstnanec má z okolností povinnost jej očekávat),
- monitorování je nasazeno na základě konkrétního podezření svědčícího o protiprávních aktivitách zaměstnance

K výše uvedeným ještě mohou přistoupit zvláštní případy, kdy je monitorovacích nástrojů užito přímo orgány veřejné moci nebo kdy k jejich užití zaměstnavatele orgán veřejné moci zaváže vrchnostenským aktem.

116 Viz např. Bernstein, A. What We Talk About When We Talk About Workplace Privacy, Louisiana Law Review, roč. 66, číslo 4, str. 923, ke stažení on-line na adrese http://digitalcommons.law.lsu.edu/lalrev/vol66/iss4/2.

117 Viz např. Selmi, M. Privacy for the Working Class: Public Work and Private Lives, Louisiana Law Review, roč. 66, číslo 4, str. 1035.

118 Srov. Rustad, M. L., Paulsson, S. R. Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe, University of Pennsylvania Journal of Labor and Employment Law, roč. 7, str. 829.

Vědomí zaměstnance o možnosti zaměstnavatele monitorovat jeho soukromou sféru na pracovišti je samozřejmě možno založit i náležitou informací. Může se pak v tomto směru jevit z pohledu zaměstnavatele jako spolehlivé řešení, pokud prokazatelně o existenci monitorovacího nástroje zaměstnance poučí nebo pokud si dokonce s jeho užitím sjedná se zaměstnancem souhlas.

Informace o monitorování soukromé sféry na pracovišti, ať už je obsažena v oběžníku nebo v interní instrukci, ani výslovná dohoda s pracovníkem ohledně toho, že s monitorováním souhlasí, však z právního hlediska nemusí mít při případném sporu žádnou zásadní relevanci. Je totiž třeba předpokládat, že pracovník je vzhledem k zaměstnavateli ve slabším postavení, které se mimo jiné projeví tím, že pravděpodobně nebude z obav o ztrátu zaměstnání nebo o šikanu ze strany zaměstnavatele odpírat udělení souhlasu nebo protestovat proti monitorovacímu nástroji, o jehož používání byl spraven[119]. Souhlas nebo jednostranná informace tedy může z právního hlediska založit zaměstnavateli právo pouze na použití takových monitorovacích nástrojů, které sice zaměstnanec nemá povinnost přímo předpokládat, ale jejichž užití zároveň nepředstavuje exces vzhledem ke standardnímu fungování příslušného pracoviště. Typickým příkladem může být instrukce, kterou zaměstnavatel informuje zaměstnance bankovní přepážky o tom, že jsou tato pracoviště nejen snímána bezpečnostními kamerami (to může pracovník vzhledem k situaci předpokládat i bez specifické informace), ale že je zde zároveň pořizován prostorový zvukový záznam.

119 České pracovní právo je z tohoto důvodu k jednostranným aktům zaměstnavatele i k dohodám omezujícím práva zaměstnanců velmi nekompromisní – srov. § 4a zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

4 PERSPEKTIVY DALŠÍHO VÝVOJE ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Shora provedená analýza má, jak bylo na několika místech zvlášť zdůrazněno, pouze doktrinální charakter a bez specifické judikatury nelze konstatovat konkrétní tvar jednotlivých institutů aktuálně tvořících českého právo kybernetické bezpečnosti. I v případě právních nástrojů, které již máme v našem právu k dispozici, totiž není jasno v tom, jaké formy může mít jejich aktuální aplikace. Diskutovat za této situace možnosti dalšího vývoje našeho práva kybernetické bezpečnosti je tedy podobno věštění z kávové sedliny.

Následující výklad je zaměřen především na možnosti dalšího vývoje české legislativy, přičemž vychází kromě shora diskutovaného současného stavu též z tendencí patrných v zahraničních právních řádech. České právo má v této souvislosti určitou výhodu spočívající v tom, že máme přístup k dobrým i špatným zkušenostem s různými typy legislativních nástrojů ze států, pro které kybernetická bezpečnost představovala a představuje v porovnání s naší situací daleko naléhavější problém. Můžeme se tedy díky spojeneckým svazkům a tradičním přátelským vazbám poučit ze zkušeností realizovaných v podobném právním prostředí, tj. v situaci standardního demokratického právního státu, ve státech, které kvůli své velikosti nebo zahraničněpolitické aktivitě staly se terčem závažných kybernetických útoků dříve a ve větší míře, než je tomu u nás.

Skutečnost, že v případě USA, Spojeného království nebo například Izraele jde o země fungující na jiných právně-kulturních základech, v tomto případě nebrání vzájemnému srovnání a využití příslušných zkušeností a dalších právních poznatků. Technika fungování právních mechanismů příslušné právní kultury totiž vzhledem k nastavení právních nástrojů pro zajištění národní kybernetické bezpečnosti není nikterak podstatná - hlavní roli při posuzování použitelnosti určitého přístupu, nástroje nebo institutu hraje zde spíše příbuznost hodnotových základů příslušných právních kultur, jimiž jsou v případě českém i v případě právě jmenovaných zemí shodně priorita práv člověka a základní principy demokratického právního státu.

Příkladem takové zkušenosti, která nám ušetřila čas a nemalé zdroje finanční, personální i politické, je původní záměr severoamerické vlády koncipovat národní úpravu kybernetické bezpečnosti na bázi identifikace útočníka[120]. Jedná se o jeden ze dvou způsobů, jak strategicky nastavit právní instituty chránící veřejný zájem na fungování kritické informační a komunikační infrastruktury, který však je vysoce problematický vzhledem k proporcionalitě práv uživatelů služeb informační společnosti (v USA není sice zakotveno právo na ochranu osobních údajů a ochrana soukromí má poněkud jiný charakter než v Evropě, ale právo na anonymní vystupování v prostředí informačních sítí je i tak extrémně silné díky prvnímu dodatku americké ústavy). Politická neprůchodnost tohoto přístupu posloužila nám za vodítko při stanovení základní strategie české resp. evropské právní úpravy kybernetické bezpečnosti, která je namísto zmíněného modelu postavena na strategické prioritě ochrany prostředí[121] s tím, že identifikace a postih útočníka je ponechán na režimu běžného fungování trestního práva resp. na standardní působnosti orgánů činných v trestním řízení.

4.1 Zákonná typologie uživatelů vybraných systémů a sítí

Z právě uvedeného plyne, že individuální odpovědnost koncového uživatele, ať je jím útočník nebo i jen subjekt, jehož systém se z nějakého důvodu podílí na kybernetickém bezpečnostním incidentu, představuje politicky velmi citlivou otázku. Předpokladem uplatnění individuální odpovědnosti uživatele, ať už má jít o odpovědnost soukromoprávní nebo trestní, je totiž jeho ztotožnění. To přitom vyžaduje použití takových mechanismů, které mohou obecně ohrozit shora zmíněnou anonymitu (jako nutnou komponentu práva na svobodu projevu) a mohou být především kontradiktorní s kategorickými požadavky výjimečně rigorózně nastavené evropské ochrany soukromí a osobních údajů.[122]

120 Srov. Sales, S. A. Regulating Cyber-Security, Northwestern University Law Review, roč. 107, číslo 4, str. 1503.

121 K tomu viz např. věcný záměr zákona o kybernetické bezpečnosti nebo průvodní dokumentaci k návrhu směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM/2013/048 final - 2013/0027 (COD).

122 Z aktuální rozhodovací praxe Soudního dvora můžeme vybrat například případy C-203/15 Tele2 Sverige AB v. Post-och telestyrelsen a C-698/15 Secretary of State for the Home Department v. Tom Watson a další.

Právě ochrana soukromí, osobních údajů, svobody projevu či obecně vzato práva na informační sebeurčení jsou důvodem toho, že se zřejmě v dohledné době nesetkáme s ničím takovým, jako internetový občanský či řidičský průkaz. Na druhé straně však je možno uvažovat o proporcionální ochraně vitálních zájmů na fungování kritických součástí informační a komunikační infrastruktury prostřednictvím specifické individuální odpovědnosti lidí, kteří na profesionální bázi s kriticky důležitými informačními systémy nebo sítěmi pracují.

Jednou z možností legislativního řešení je maďarský model definice stupňů bezpečnostní důležitosti informačních systémů a sítí a založení práva pracovat s těmito systémy pouze uživatelům s určitým stupněm znalostní certifikace[123]. Nemusí přitom jít pouze o povinnost pro správce příslušného systému nebo sítě spočívající v nutnosti proškolit své zaměstnance respektive najmout si pro jejich obsluhu odborně náležitě vybavený personál. Zprostředkovaně může jít též o vytvoření specifických povinností na straně samotného uživatele založených předpisy na úseku kybernetické bezpečnosti, zakládajících správní odpovědnost za přestupky nebo jiné správní delikty spočívající v neodborném přístupu ke kriticky důležitým systémům nebo sítím a odstupňované adekvátně k jejich bezpečnostní klasifikaci.

Je docela pravděpodobné, že potřebu takové úpravy pocítí v první řadě především správci kritické informační a komunikační infrastruktury poté, co konstatují nutnost až příliš sofistikované tvorby interních instrukcí tak, aby bylo v případě problému na straně uživatele nebo operátora kriticky důležitého systému nebo sítě možno regresně vyvodit alespoň disciplinární odpovědnost. Problémem interních instrukcí totiž je, že jejich závaznost či praktická vynutitelnost není jen otázkou jejich bezrospornosti se zákonem, ale též jejich srozumitelnosti a formy komunikace (viz výše). Byť to může znít na první pohled poněkud problematicky, je proto pro zaměstnavatele nepoměrně jednodušší, pokud se může spolehnout na zákonnou nebo podzákonnou definici konkrétních bezpečnostních povinností svých zaměstnanců, než pokud by takovou definici měl sám vytvářet a implementovat. Individuální správní odpovědnost je navíc sama o sobě silným motivačním

123 Srov. maďarský zákon o elektronické informační bezpečnosti ústředních a místních správních orgánů ze dne 15. dubna 2013 – ke stažení v anglické verzi on-line na adrese http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx.

faktorem, který může pro příslušné zaměstnance představovat ještě pádnější důvod k obeznámení se s bezpečnostními pravidly a k jejich dodržování, než je tomu v případě disciplinární odpovědnosti nebo omezené odpovědnosti za škodu způsobenou zaměstnavateli.

Ve vazbě k výše uvedenému je možno uvažovat též o zákonem založené povinnosti pro správce vybraných typů vysoce bezpečnostně exponovaných informačních systémů a sítí vyčlenit resp. zaměstnat pracovníka přímo odpovědného za plnění požadavků zákona o kybernetické bezpečnosti. Podobně, jako je tomu v agendě ochrany utajovaných informací[124] nebo v některých členských státech v agendě ochrany osobních údajů[125], mohl by tento zaměstnanec mít v organizační struktuře příslušného správce ze zákona dané specifické postavení a jeho disciplinární odpovědnost by mohla být rozdělena mezi zaměstnavatele a národního regulátora (tj. v našem případě zřejmě Národní bezpečnostní úřad).

4.2 Omezená odpovědnost běžných uživatelů

Nejen z politických důvodů je zřejmě nereálné předpokládat, že by právní úprava kybernetické bezpečnosti v dohledné době specificky založila objektivní odpovědnost koncových uživatelů nebo zavedla nějaký zvláštní mechanismus jejich identifikace. Přes všechny více či méně argumentované požadavky na to, aby uživatelé odpovídali za bezpečné fungování svých systémů bez ohledu na své zavinění, je totiž třeba v první řadě zohlednit skutečnost, že i relativně jednoduché technologie určené k běžnému použití v domácnostech (typicky např. mobilní telefony, domácí wifi routery apod.) jsou z podstaty extrémně technicky složité. Běžný uživatel tedy nejenže nechápe (resp. nemusí chápat) ani základní principy jejich fungování, ale nelze po něm požadovat ani to, aby se zvlášť věnoval jejich zabezpečení proti možnému zneužití. Jestliže tedy prostý spotřebitel např. neprovede instalaci bezpečnostní záplaty a v důsledku toho je jeho systém zneužit k útoku typu

124 Srov. § 71 zákona č. 412/2005 Sb.

125 Povinnost zřídit u větších subjektů tuto funkci se plánuje k celoevropskému zavedení v nové úpravě evropské ochrany osobních údajů – k tomu viz k tomu viz Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

DDoS, není v dohledné době možno uvažovat o tom, že by za takový útok měl nést spoluodpovědnost.

Z hlediska proporcionality dotčených práv nesrovnatelně schůdnějším řešením by byla regulace spotřebitelské dostupnosti informačních a komunikačních technologií v závislosti na míře jejich bezpečnosti. Lze tedy uvažovat o tom, že budou pro určité typy informačních a komunikačních technologií zavedeny mandatorní požadavky na jejich kvalitu, které zahrnou i nutnou jejich bezpečnostní výbavu. Podobně, jako je tomu pravidlem v síťových odvětvích, tj. např. v energetice, telekomunikacích nebo v dopravě, může i v oblasti kybernetické bezpečnosti vzniknout katalog požadavků na shodu, který zahrne nejnutnější bezpečnostní prvky a bez jejichž dodržení nebude možno příslušnou technologii spotřebitelsky šířit na tuzemském trhu. I v tomto případě by šlo zprostředkovaně o zatížení koncového uživatele – nikoli sice přímými povinnostmi či odpovědností, ale nutností zaplatit příslušné zabezpečení včetně jeho administrativních externalit v konečné ceně produktu nebo služby. Takové řešení je však stále z hlediska ochrany práv nesrovnatelně schůdnější, než shora diskutovaná objektivní odpovědnost.

Možnost, jak ústavně konformním způsobem založit nepřímou odpovědnost koncových uživatelů ukázal výše diskutovaný případ Microsoft. Tento případ není pro českou právní praxi inspirativní do té míry, že by bylo snad možno uvažovat o podobném řešení v našich podmínkách. Naše procesní právo totiž nedovoluje žalovat na základě identifikačního znaku, nelze-li podle něj přímo v řízení ztotožnit konkrétní subjekt. I pro naše právní prostředí je však zajímavá úvaha soudu ohledně toho, že i běžný uživatel má určitou míru povinnosti vědět o potřebě zabezpečení svého vlastního systému a že tuto povinnost lze uvést do souvislosti s adekvátním typem odpovědnostního následku, tj. nikoli např. hradit škodu ale „pouze" strpět dálkový zásah do svého systému.

Prostředkem, který by bylo možno využít namísto shora popsaného řešení, mohlo by se stát opatření obecné povahy. To totiž umožňuje identifikovat své adresáty na základě obecných znaků a uložit jim určitou povinnost. Je pak možno svěřit konkrétnímu úřadu (v našem případě by zřejmě šlo o Národní bezpečnostní úřad nebo Český telekomunikační úřad) kompetenci vydávat za přesně stanovených okolností tato opatření a ukládat jimi i běžným (nic

netušícím) uživatelům podobné povinnosti strpět zásah do jejich systémů, jako se stalo ve shora zmíněném případě.

4.3 Specifická úprava outsourcingu

Jádrem aktuální zákonné úpravy i podzákonných prováděcích předpisů v oblasti kybernetické bezpečnosti jsou bezpečnostní opatření. Požadavky na standard zabezpečení informační a komunikační infrastruktury spravované povinnými subjekty jsou zákonem stanoveny velmi obecně a prováděcí předpisy pak obsahují jen takovou míru jejich konkretizace, která nezasahuje do principu technologické neutrality a umožňuje povinným subjektům autonomii při volbě konkrétních řešení. Tento model jeví se jako vhodný hned ze dvou důvodů – předně je povinný subjekt tím nejvíce povolaným, pokud jde o detailní technické znalosti příslušného informačního systému nebo sítě a má tedy nejlepší možnost posoudit, jaká konkrétní bezpečnostní řešení nejlépe splní zákonné požadavky. Vedle toho je velmi pravděpodobné, že relativní otevřenost standardních požadavků povede společně s jistotou investic k motivaci dodavatelů různých bezpečnostních řešení k investicím do vývoje. To může přinést vítaný impuls k dalším inovacím v oboru ICT bezpečnosti.

Relativně velká míra autonomie u povinných subjektů ohledně způsobu plnění zákonných požadavků však na druhé straně vyvolává i nejistotu ohledně řešení typických případů, kdy správce nerealizuje jednotlivá bezpečnostní opatření sám nebo alespoň ve vlastní režii, ale provádí jejich komplexní outsourcing. Především u středně velkých a menších povinných subjektů lze kromě vzájemné koordinace jejich aktivit při akvizicích bezpečnostních řešení očekávat i společné postupy při komplexním řešení bezpečnostních opatření včetně jejich fungování v reálném čase. Lze si tedy například představit, že místní utility typu vodáren nebo tepláren vytvoří společný podnik, který bude jim bude zajišťovat realizaci a fungování bezpečnostních opatření např. i včetně provozu lokálního CERT, reportování incidentů, spolupráce s národním nebo vládním dohledovým pracovištěm apod.

Zákon a podzákonné předpisy sice možnost outsourcingu bezpečnostních opatření nevylučují a v konkrétních částech s ní přímo počítají. Pravidla pro externí dodavatele bezpečnostních řešení však se omezují pouze na obecné povinnosti mít dokumentovány a kontrolovány vztahy s externími dodavateli.

Vzhledem k tomu, že zákon o kybernetické bezpečnosti stojí na výlučné odpovědnosti správce příslušného informačního systému nebo sítě, není v jeho současné struktuře obsažena speciální úprava postavení dodavatele nebo provozovatele bezpečnostních opatření. Je tedy plně na správci, jak si vztahy s externími subjekty vyřeší a jak bude ve vztahu k nim zajišťovat například plnění povinností vyplývajících z kontrolních pravomocí Národního bezpečnostního úřadu nebo regresní nároky v případě deliktní odpovědnosti.

Zatímco volnost ve smyslu konkrétní formy bezpečnostních opatření jeví se jako vhodná a není důvod předpokládat v brzké budoucnosti nějaké zásadní změny, je otázku totální volnosti povinných subjektů ohledně outsourcingu bezpečnostních opatření možno považovat za místo, kde bude zákonná úprava průběžně doplňována na základě praktických zkušeností. Nejde pouze o možnost založení přímých pravomocí Národního bezpečnostního úřadu vůči subjektům poskytujícím bezpečnostní řešení jako službu, ale například i o možnost správní regulace činnosti takových subjektů (nabízí se například varianta speciální vázané živnosti). Především ve vztahu k informačním systémům veřejného sektoru spadajících pod rozsah zákona o kybernetické bezpečnosti (tj. k informačním systémům veřejné správy a dalším informační systémům provozovaným veřejnoprávními korporacemi, které budou spadat pod rozsah kritické informační infrastruktury nebo významných systémů) lze očekávat i podrobnější úpravu požadavků na outsourcing, která by měla odstranit standardní bezpečnostní nešvary vyskytující se v procesech zadávání veřejných zakázek na ICT.

Vedle konkrétnější úpravy zákonných a podzákonných parametrů outsourcingu bezpečnostních opatření lze předpovědět i nepoměrně rychlejší vývoj smluvních nástrojů a alternativních forem řešení obchodních sporů, a to především u soukromoprávních povinných subjektů. Dokonce ještě před platností (nikoli až účinností) zákona o kybernetické bezpečnosti byly některé velké korporace včetně energetických společností nuceny zahrnovat do outsourcingových smluv klauzule zakládající pro dodavatele resp. poskytovatele služby specifické povinnosti v návaznosti na budoucí zákonné bezpečnostní požadavky.

Konstrukce těchto klauzulí, kontrola příslušných plnění v reálném čase (může totiž jít o mnohaleté smlouvy) nebo mechanismy řešení vzájemných sporů představují oblast smluvního ICT práva, která sice u nás není úplně zanedbána, bude však zřejmě ještě procházet velkým rozvojem. Namísto legislativní asistence však je v tomto směru spíše nutno očekávat, že si budou muset soukromoprávní povinné subjekty, zjednodušeně řečeno, pomoci samy – přispět ke zdárnému vývoji smluvních nástrojů, procedur výběru dodavatelů nebo procedur řešení dodavatelských sporů mohou kromě organizací typu Hospodářské komory především oborové asociace. Kvalitně fungující vztahy s dodavateli bezpečnostních opatření totiž nepředstavují otázku vzájemné konkurence mezi subjekty působícími na týchž trzích a přímo se tak nabízí vzájemná bezkonfliktní spolupráce a koncentrace zdrojů k zajištění efektivně fungujících právních řešení.

4.4 Další vývojové perspektivy práva kybernetické bezpečnosti

K právě uvedenému lze spekulativně připojit i další oblasti, z nichž na prvním místě se bude zřejmě jednat o postupnou národní i mezinárodní konkretizaci pojmu informační suverenity státu. Primárním těžištěm tohoto problému bude zřejmě mezinárodní právo veřejné a výstupy můžeme očekávat především z jeho doktríny. Přestože ideálním řešením by v tomto směru byla mezinárodní úmluva, nedá se vzhledem ke zcela rozdílným pohledům na věc a zcela odlišným zájmům jednotlivých národních vlád očekávat, že by k přípravě takové úmluvy mohlo v dohledné době dojít. Příliš pravděpodobný není ani vznik judikatury Mezinárodního soudního dvora, neboť státy, které by toho byly schopny, nemají, stručně řečeno, k přednesení aktuálně se vyskytujících konfliktních situací tomuto fóru prakticky žádnou motivaci. Namísto toho je spíše důvod očekávat další rozvoj vzájemné spolupráce na základě existujících obecných spojeneckých svazků, z nich nejvýznamnější a doposud nejproduktivnější je spolupráce v rámci NATO[126].

[126] Z doktrinálního hlediska nejvýznamnější výstupem této spolupráce je činnost centra excelence CCD CoE v estonském Talinu, jejíž manuál se stal všeobecně uznávaným standardem doktríny mezinárodního práva veřejného pro kybernetickou bezpečnost. Manuál je on-line ke stažení ze http://issuu.com/nato_ccd_coe/docs/tallinnmanual.

Nesrovnatelně jednodušší je co do synergie základních hodnot a zájmů situace v rámci Evropské unie. Vedle postupné implementace směrnice NIS lze tedy čekat i další rozvoj stávajících a další rozvoj stávajících evropských bezpečnostních struktur, zejm. ENISA a CERT-EU. V českém právním prostředí můžeme nad rámec toho, co bylo diskutováno v předchozích kapitolách, očekávat především konkretizaci spolupráce vládního a národního CERT, jakož i konkretizaci spolupráce Národního bezpečnostního úřadu s ostatními orgány veřejné moci, do jejichž zájmu spadá oblast národní kybernetické bezpečnosti (vedle bezpečnostních služeb jde především o Policii ČR, Armádu ČR a ústřední orgány státní správy mající jurisdikci nad kritickými či významnými informačními systémy a sítěmi)[127]. Podobně lze očekávat též rozvoj spolupráce mezi Národním bezpečnostním úřadem a soukromoprávními korporacemi, profesními sdruženími a akademickou sférou – ta může mít charakter neformálních aktivit, memorand, činnosti expertních skupin apod. a může řešit problémy, které z nějakého důvodu není možno nebo vhodno pokrýt veřejnoprávními aktivitami (typicky např. otázky certifikace, vzdělávání, podpory inovací apod.)

Jako nanejvýš vhodná jeví se v tomto směru být tendence zahrnovat kybernetickou bezpečnost mezi aktuální politické priority – to umožní podporovat shora uvedené činnosti v rámci standardních forem spolupráce mezi soukromým, akademickým a veřejným sektorem typu podpory vědeckých nebo rozvojových projektů, exportu, investic, rozvoje občanské společnosti aj.

127 Národní bezpečnostní úřad již v tomto směru publikoval několik podpůrných dokumentů jako např. blokové schéma zákona o kybernetické bezpečnosti nebo pomůcky k určení prvku kritické informační infrastruktury a významných systémů – dokumenty jsou ke stažení on-line na adresách: www.govcert.cz.

5 PERSPEKTIVY DALŠÍHO POLITICKÉHO A ORGANIZAČNÍHO VÝVOJE AGENDY KYBERNETICKÉ BEZPEČNOSTI V ČR

5.1 Certifikace a compliance check

Jak uvedeno shora, pracuje návrh české právní úpravy s principem autonomie vůle regulovaných subjektů. Jedním z projevů tohoto principu ve spojení s principem technologické neutrality je mandatorní stanovení cílových charakteristik bezpečnostních opatření (organizačních i technických) a ponechání konkrétní formy realizace na úvaze příslušného povinného subjektu. Vhodnost takového řešení je vedle obecně menší regulatorní zátěže pro povinné subjekty dána též skutečností, že příslušné bezpečnostní řešení může být vždy realizováno na míru konkrétního systému. Regulovaný subjekt má tedy praktickou volnost ve výběru architektury, technologie i dodavatelů.

Určitou nevýhodou tohoto jinak vhodně zvoleného řešení však je skutečnost, že povinné subjekty budou mít jen omezenou míru právní jistoty ohledně otázky, zda právě jejich konkrétní řešení odpovídá zákonným požadavkům, tj. zda v případě kontroly ze strany Národního bezpečnostního úřadu nebudou shledány vzhledem k zákonným požadavkům nějaké nedostatky. Byť jsou totiž požadované parametry bezpečnostních opatření definovány s maximální mírou určitosti, nelze se, a to ani při konkretizaci jednotlivých parametrů formou podzákonných právních předpisů, ubránit relativně velké míře abstrakce a výsledné nejistoty plynoucí vedle relativně abstraktních zákonných a podzákonných pojmů též z velkého množství různých organizačních a technických kritérií.

K relativní neurčitosti zákonných resp. podzákonných požadavků pak ještě přistupuje určitá míra nejistoty ohledně implementace a následného provozu bezpečnostních opatření. Zákonné požadavky totiž nesměřují jen ke statické formě bezpečnostních opatření (tj. k jejich statickým formálním parametrům) ale též k jejich implementaci a fungování v reálném čase.

I bezpečnostní řešení dostatečně dimenzované vzhledem k zákonným požadavkům totiž může ve svém výsledku porušovat zákonné podmínky kvůli neadekvátní implementaci nebo nedostatečné pozornosti vzhledem k jeho trvalému provozu.

Nejistota ohledně toho, zda projektované, pořízené, implementované a provozované bezpečnostní řešení splňuje zákonné parametry, představuje závažný problém především pro střední a velké podniky, jakož i pro veřejnoprávní korporace. U středních a velkých podniků jedná se především o otázku compliance, přičemž především nadnárodní korporace často řeší otázky a priori plnění zákonných požadavků v příslušných jurisdikcích jako naprostou prioritu. Aktuálně se to týká např. otázek ochrany osobních údajů, bezpečnosti práce, požární bezpečnosti, utajovaných informací apod. Pro podnik velkého rozsahu je totiž zásadně důležité vyčíslení nákladů na plnění právních povinností v příslušné jurisdikci a priori – jen tak s nimi totiž lze kalkulovat do finančních plánů. Situace, kdy je velká nebo střední korporace nucena kalkulovat potenciální náklady na plnění právních povinností a posteriori, vždy generuje značnou míru nejistoty, neboť právní odpovědnost (postih) se v komplexních případech jen velmi těžko odhaduje a těžké je i provést takovou kalkulaci do všech možných důsledků (k tomu viz výše).

V případě naší právní úpravy kybernetické bezpečnosti tak jde příkladně o to, jaké mohou být právní následky implementace a používání takového systému bezpečnostních opatření, o kterém se následně prokáže, že nesplňuje zákonné požadavky. U velkého nebo středního podniku je v tomto směru případná pokuta jen jedním z mnoha možných následků, neboť nezákonnou implementací mohou být způsobeny např. škody třetím osobám nebo může v důsledku nařízených opatření k nápravě dojít k omezení provozu či k potřebám zásadních organizačních změn.

Dokonce i tam, kde lze počítat s konkrétní výší např. pokut, náhrad škody nebo škod způsobených zastavením nebo omezením provozu, představuje u všech typů podnikatelských subjektů a posteriori řešení právní rizikovosti velmi nevítanou alternativu. Není totiž žádným tajemstvím, že podnikatelské aktivity mohou být významně poškozeny už tím, že se orgány státní moci nějakou formou o příslušný podnik zajímají. Typicky pak může

i pouhá kontrola nebo vyšetřování ze strany oprávněných orgánů státní moci způsobit jen těžko předvídatelné komplikace a vést ke ztrátám, jejichž hodnotu lze jen stěží předem vyčíslit. To platí samozřejmě i pro případy, kdy vyšetřování nebo kontrola nevedou ve vztahu k příslušnému orgánu veřejné moci k žádném sankčnímu důsledku, neboť i pouhá vrchnostenská přítomnost na kontrolovaných pracovištích může se negativně projevit na výkonu celého podniku.

U veřejnoprávních korporací je otázka a priori souladu s požadavky právního řádu ještě důležitější než u podnikatelských subjektů. V porovnání se soukromoprávními subjekty jde dokonce o prioritní otázku bez ohledu na jejich velikost. Je-li totiž k pořízení nebo provozu bezpečnostních opatření užito veřejných prostředků, nelze riskovat dodatečnou kvalifikaci těchto opatření jako nesouladných se zákonnými požadavky.

Lze navíc předpokládat, že investice veřejného sektoru do kybernetické bezpečnosti budou minimálně z podstatné části kryty prostředky z různých rozvojových projektů – příjemce takových prostředků si pak dvojnásob nemůže dovolit rizikovost investice vzhledem ke splnění zákonných požadavků resp. nemůže si dovolit riskovat situaci, kdy projektové prostředky použije způsobem, který je dodatečně (např. na základě kontroly) označen za nikoli souladný s platnou právní úpravou. Poskytovatel dotace má totiž v takovém případě právo či dokonce povinnost dovolávat se podmínek jejího poskytnutí a požadovat vrácení poskytnutých prostředků.

Z právě popsaných důvodů lze mezi středními a velkými soukromoprávními subjekty a veřejnými korporacemi očekávat velkou poptávku po a priori aprobačních procedurách poskytujících nezávislé ujištění ohledně toho, že implementované resp. provozované řešení bezpečnostních opatření je v souladu s požadavky účinné právní úpravy. Objektivně ideální variantou řešení tohoto problému by byla zákonná certifikační procedura realizovaná přímo příslušným orgánem státní exekutivy (v českém právním prostředí zřejmě Národním bezpečnostním úřadem) nebo jím pověřeným a dozorovaným nezávislým expertním pracovištěm.

Skutečnost, že taková procedura není součástí struktury navrhované právní úpravy, však lze jen sotva vnímat jako chybu právotvůrce nebo jako pravou mezeru v právu. Taková procedura musela by totiž být podrobně a rigorózně

upravena, aby nevzniklo riziko privatizace výkonu nedistributivních práv resp. aby nebyl indukován korupční potenciál. Je přitom jen velmi obtížné takovou rigorózní úpravu provést v situaci, kdy jsou k dispozici v tomto ohledu jen velmi omezené zkušenosti (zde je nutno připomenout, že stávající komerční certifikační procedury zaměřují se především na problematiku organizačních opatření, nikoli už na technologie k zajištění kybernetické bezpečnosti nebo na spolupráci s centrálními dohledovými pracovišti).

Zavedení státní certifikace by rovněž vyžadovalo důkladnou přípravu institucionální a personální a je třeba v tomto směru konstatovat, že na našem pracovním trhu zdaleka není přebytek pracovní síly disponující dostatečnou mírou kvalifikace v oboru kybernetické bezpečnosti a k tomu náležitě motivované za aktuálních platových podmínek ke vstupu do služeb státu. Příprava adekvátní procedury by tedy z hlediska organizačního i personálního vyžadovala takovou časovou a finanční dotaci, kterou si vzhledem k vývoji bezpečnostní situace nemůže v současné době Česká republika dovolit (kromě toho je třeba po bohatých našich zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).

Ve prospěch státního řešení certifikace může naopak hovořit pozitivní zkušenost s obdobnou procedurou v agendě ochrany utajovaných informací. Ani v tomto případě přitom nebylo možno ji realizovat okamžitě, ale příslušné kapacity se postupně vytvářely. Skutečnost, že v tomto případě nejde o korupčně exponovanou situaci, navíc ukazuje, že je v případě Národního bezpečnostního úřadu možno předpokládat takovou kvalitu institucionálních opatření, která vzniku a rozvoji korupčního rizika účinně brání. V případě kybernetické bezpečnosti by navíc bylo možno v porovnání s technologiemi a postupy pro ochranu utajovaných informací učinit celý certifikační proces ještě transparentnějším (tj. vystavit jej ve větší míře veřejné kontrole v tomto případě vykonávané především dodavateli vzájemně konkurenčních bezpečnostních řešení) a lze tedy konstatovat, že korupční rizikovost by bylo možno v takovém případě prakticky vyloučit.

Problémem však každopádně zůstává shora konstatovaná a jen těžko okamžitě řešitelná dlouhodobost náběhu veřejnoprávní certifikační procedury daná nutností vytvořit na straně NBÚ odborně zdatný a dostatečně robustní

personální substrát[128]. Jedinou variantou přímého zapojení orgánu veřejné moci do a priori certifikace bezpečnostních řešení tedy zůstává institucionální nebo produktová aprobace certifikační procedury realizované nezávislým subjektem s dostatečnou personální kapacitou, tj. akademickou institucí, profesním či oborovým sdružením nebo komerčním poskytovatelem.

Role zájmových sdružení a organizací zajišťujících expertní spolupráci soukromého a veřejného sektoru je v tomto směru zřejmě klíčová. Ve vzájemné spolupráci s orgány odpovědnými za výkon vrchnostenské správy na úseku kybernetické bezpečnosti a nezávislými akademickými institucemi mohou tyto organizace pomoci s vytvořením nezávislých certifikačních procedur praeter legem, které nebudou mít vrchnostenský charakter, ale přesto poskytnou zájemcům z řad soukromého a veřejného sektoru nezávislé komplexní posouzení jejich bezpečnostních opatření vzhledem k zákonným a podzákonným požadavkům. Charakter zájmového sdružení v tomto případě kombinuje aspekt transparentnosti (tj. je jasné, že jde o aktivitu obchodní komunity) a profesní specializaci (tj. zaměření na konkrétní ekonomické odvětví) s legitimitou společného postupu, tj. nejde pouze o zájem jednoho podnikatele, ale aktivita sdružení odráží vůli jinak si vzájemně konkurujících subjektů.

Takové certifikační procedury samozřejmě nebudou disponovat vrchnostenským charakterem a jejich výstupy nebudou zavazovat orgány veřejné moci při hodnocení souladu příslušných bezpečnostních řešení se zákonem a podzákonnými předpisy. Při nalezení adekvátního modelu spolupráce s vrchnostenskými orgány však lze tímto prostřednictvím docílit faktické akceptace těchto certifikačních procedur alespoň v procesním smyslu. Jinými slovy tedy takový certifikát nemůže sice absolutně ochránit příslušný subjekt před kontrolou nebo následnou sankcí, jeho udělení však může být při případné kontrole fakticky zohledněno. Zatímco tedy může být za běžných podmínek prováděna kontrola bezpečnostních opatření bez jakékoli presumpce, může Národní bezpečnostní úřad kontrolovat certifikovaná bezpečnostní řešení s presumpcí souladu. Takové procesní řešení může pak

128 S tímto problémem se každopádně nepotýká jen Česká republika – srov. Devost, M. G., Moss, J. Pollard, N. A. Stratton, R. J. III. All Done Except the Coding, Georgetown Journal of International Affairs, roč. 11, str. 197 a násl.

pragmaticky posloužit nejen povinným osobám, ale samotnému Národnímu bezpečnostnímu úřadu – logicky ale jeho implementace vyžaduje především vzájemnou důvěru, kterou může zajistit pouze skutečná nezávislost certifikační procedury, jakož i její vysoká odborná úroveň. Obojí je v našem prostředí řešitelné v první řadě spoluprací s renomovanými akademickými institucemi.

Především z hlediska povinných subjektů užívajících k investicím do pořízení nebo provozu bezpečnostních opatření veřejné prostředky (v tomto případě je lhostejno, zda jde o soukromoprávní nebo veřejnoprávní organizace) je shora popsané řešení vhodné i z důvodu možné inkorporace do zadávací dokumentace resp. do mandatorních požadavků na dodavatelská řešení. Namísto relativně neurčitých formulací ohledně souladu bezpečnostních opatření s platnou právní úpravou budou tyto subjekty moci v implementačních nebo realizačních smlouvách využít ujednání odkazující na získání konkrétních typů certifikací a sjednat si tím vyšší míru právní jistoty. Obdobná může být též situace u dlouhodobých outsourcingových kontraktů, kde požadavek na certifikaci příslušného bezpečnostního řešení na aktuálně účinný standard může být na straně odběratele adekvátně řešit jistotu ohledně průběžného plnění zákonných resp. podzákonných povinností, u nich lze oprávněně očekávat, že se budou v čase výrazně vyvíjet a měnit (k tomu viz výše).

K právě uvedenému je nutno doplnit, že příslušná certifikační řešení zdaleka nemusí být unikátní nebo monopolní resp. že pro různé typy bezpečnostních řešení mohou fungovat různé procedury. Certifikace tak může být prováděna např. formou prověrky ve fázi projektu informačního systému nebo sítě, kontroly jeho implementace nebo provozních zkoušek jako součásti různých fází akceptace příslušných dodávek. Formu certifikace mohou mít též například i penetrační testy nebo jiné typy operačních prověrek běžících systémů nebo sítí. Tento model může být využíván především u dlouhodobých outsourcingových kontraktů, přičemž odběratel může mít díky němu stálou kontrolu nad kvalitou dodávané služby a nad skutečností, že služba např. i po několika letech stále plní aktuální požadavky právní úpravy (v tomto směru je třeba připomenout relativně vysokou pravděpodobnost postupných změn požadavků na bezpečnostní opatření v návaznosti

na obecný technický vývoj). Certifikací mohou konečně procházet vedle celých bezpečnostních řešení i jen dílčí systémy nebo dokonce jejich jednotlivé komponenty – typicky tak může být systém nebo síť podrobena experimentální bezpečnostní expozici v testovacím polygonu a na základě kvality její odezvy může být certifikační autoritou doporučena/nedoporučena pro nasazení v určitém typu informačního systému nebo sítě.

Vzhledem k tomu, že bezpečnostní opatření mohou být dle platné právní úpravy šita přímo na míru konkrétním systémům nebo sítím, je vhodné podporovat i takové certifikační iniciativy, které budou směřovány do konkrétních hospodářských resp. veřejnoprávních sektorů[129]. Lze očekávat, že profesně resp. sektorově orientované iniciativy mohou být v tomto směru mnohem efektivnější – je přitom logické, že typická bezpečnostní řešení v justici se budou zřejmě na úrovni technické i organizační zásadně odlišovat od bezpečnostních opatření aplikovaných v oblasti energetických systémů a sítí. Profesně resp. sektorově orientované iniciativy mohou v tomto směru přinést ve smyslu efektivity nejen odpovídající úroveň znalostí v oboru kybernetické bezpečnosti ale také poznatky ohledně specifických požadavků v příslušném odvětví nebo oboru.

Jako problematická jeví se konečně v současné situaci též rizika plynoucí z čistě podnikatelsky orientovaných iniciativ, které může indukovat shora popsaná poptávka. Nebude-li totiž problematika a priori aprobace bezpečnostních opatření řešena formou spolupráce orgánů veřejné moci, akademických institucí a odborně orientovaných a ideálně i agregovaných soukromých iniciativ, vytvoří se tím prostředí pro živelný vznik samozvaných razítkovacích produktů. Bude pak extrémně složité dostat takový čistě ekonomicky motivovaný chaos do situace, kdy bude možno se na příslušné certifikáty či jiné formy potvrzení z odborného hlediska skutečně spolehnout. Jen těžko si pak lze představit, jaké praktické důsledky by mohla mít situace, kdy by aprobaci bezpečnostních opatření nezávisle prováděli např. jednotliví znalci (bude-li zachována současná situace ohledně podmínek pro výkon a odbornou úroveň znalecké činnosti).

---

129 Ke specifickým požadavkům v oboru energetiky viz např. Oliveira, D. Cyber-Terrorism & Critical energy Infrastructure Vulnerability to Cyber-Attacks, Environmental & Energy Law & Policy Journal, roč. 5, číslo 2, str. 519 a násl.

5.2 Aktivní obrana – best practices

K tématu aktivní obrany je nutno předeslat, že v současné době neexistuje žádná obecně uznávaná taxonomie jejích typických forem. Pokud už je téma aktivní obrany[130] předmětem odborných publikací, zaměřuje se debata buď to na technické aspekty konkrétních typů obranných opatření nebo na základní systematiku v rámci relativně úzce vymezených typů. Nelze však hovořit o žádné komplexní systematice a dokonce ani o definici, která by mohla pojem aktivních obranných opatření (aktivních protiopatření) alespoň rámcově popsat.

Za této situace je problematika aktivní obrany logicky spíše vědeckým zadáním a měla by být řešena spíše formou výzkumných aktivit a iniciativ. Jediným použitelným zárodkem obecné taxonomie aktivních protiopatření je výše diskutovaná Dagstuhlská taxonomie[131], která byla sestavena v rámci specializovaného semináře Leibnizovy nadace na podzim 2013 a reflektovala požadavky na systematiku z hlediska informatiky i právní vědy. Ani tato taxonomie však není prakticky použitená, neboť obsahuje pouze náznak základních kategorií a bude tedy nutno ji dále vyvíjet a doplňovat.

Aktuální praxe kybernetické bezpečnosti však nemůže čekat na výstupy vědeckých projektů, neboť aplikace aktivních protiopatření představuje v běžném fungování služeb informační společnosti každodenní nutnost. Vzhledem k tomu, že reálně užívaná aktivní protiopatření často zasahují do vlastnických či závazkových práv nebo dokonce naplňují formální znaky skutkových podstat trestných činů, představuje jejich uplatňování doposud šedou zónu a podnikatelé, kteří tato opatření používají, tak zpravidla činí skrytě. Dokonce ani technici vyvíjející a aplikující tato opatření na objednávku soukromoprávních subjektů často ani nejsou s těmito subjekty v žádném oficiálním právním vztahu.

130 K pojmu viz Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, Harvard Journal of Law And Technology, roč. 25, číslo 2, str. 431.

131 Viz Freiling, F. C., Hornung. G. Polcak, R. (eds.) Forensic Computing – report from Dagstuhl Seminar 13482, Dagstuhl: Dagstuhl Publishing, 2014, str. 204-205, publ. on-line na adrese http://drops.dagstuhl.de/opus/volltexte/2014/4442/pdf/dagrep_v003_i011_p193_s13482.pdf

Poněkud lepší je v tomto směru situace ve veřejném sektoru, přičemž typicky orgány výkonné moci mohou při užití aktivních protiopatření aplikovat obecná oprávnění založená jim v návaznosti na charakter chráněného zájmu. Ani v tomto případě však není situace úplně ideální, neboť při aplikaci obecných oprávnění často vyvstávají otázky ohledně rozsahu příslušných institutů. Orgány veřejné moci jsou rovněž v užití aktivních ochranných prostředků obecně omezeny mlhavými hranicemi vlastní institucionální legitimity – typicky tak armádní složky mohou užít svých extrémně širokých oprávnění pouze za situace, kdy jde o věc národní suverenity, bezpečnostní složky mohou aktivně jednat pouze v zájmu vnitřní nebo vnější národní bezpečnosti a orgány činné v trestním řízení mají manévrovací prostor vymezen agendou vyšetřování a stíhání trestných činů resp. ochranou veřejného pořádku.

Na jednoduchou otázku, jaké aktivní prostředky může užít policista zařazený do obvodního oddělení (je-li toho samozřejmě technicky schopen), když zjistí útok na web místního podnikatele, tedy neexistuje dokonce ani obecná odpověď. Podobně nejsme schopni odpovědět dokonce ani na mnohem prozaičtější otázky nemající charakter bezpečnostních problémů, typicky na otázku, jaké konkrétní aktivní prostředky lze použít při získávání elektronických důkazů z informační a komunikační infrastruktury.

Jak je však uvedeno shora, nemůžeme si dovolit reagovat na faktickou situaci jen pokrčením ramen a vývojem či tolerováním šedé zóny prakticky používaných, účinných a potřebných aktivních opatření, která však existují zcela mimo účinnou právní úpravu. Roli soukromoprávních iniciativ lze v tomto směru vidět především v komunikaci praktických potřeb a sběru a vyhodnocování informací ohledně prakticky používaných technik v různých odvětvích hospodářství a společenského života a v následném zpracovávání těchto poznatků do podoby technických resp. právovědných zadání pro další výzkum a legislativní praxi.

V porovnání se shora popsanou potřebou řešení certifikačních procedur však každopádně platí, že v otázce aktivní obrany nemáme prozatím k dispozici ani představu ohledně konkrétních potřeb a z nich vycházejících zadání pro organizační, technickou nebo legislativní realizaci. O to víc je samozřejmě nutno tuto otázku aktivně zpracovávat a řešit. V tomto směru je však nutno připomenout, že nemá smysl začít pracovat na řešení

jakýchkoli partikularit bez současné představy o smyslu a účelu aktivních protiopatření jako takových a o jejich reflexi základními principy, na nichž stojí náš právní řád.

5.3 Kybernetická bezpečnost jako agenda podpory investic

Jedním ze základních principů, na nichž stojí legitimita české právní úpravy, je princip bdělosti vzhledem k ostatním státům a mezinárodnímu společenství. Vedle shora popsané, byť stále nikoli prakticky uplatňované, částečné přičitatelnosti kybernetického útoku státu neschopnému při vynaložení rozumného úsilí zabránit zneužití informační a komunikační infrastruktury pod vlastní jurisdikcí, projevuje se tento princip i mnohem bezprostředněji, a to ve vztahu k ochraně investic. Česká republika je vázána obecnými procedurálními pravidly řešení sporů mezi státy a soukromoprávními investory doplněnými řadou bilaterálních dohod o ochraně investic zakládající pravomoc příslušných rozhodčích institucí – tato právní úprava vede ve výsledku k možnému založení odpovědnosti České republiky za investice zmařené v důsledku nelegitimního výkonu státní moci resp. v důsledku toho, že stát příslušné investice adekvátně neochrání.

Ve vztahu ke kybernetické bezpečnosti je možno konstatovat, že investor má v našich geopolitických reáliích oprávněná očekávání nejen co do fyzické bezpečnosti ale též co do obecné funkčnosti služeb informační společnosti. V případě, že stát není schopen zajistit fungující informační a komunikační infrastrukturu, jedná se z hlediska investora nejen o faktor při rozhodování o samotné lokalizaci investice ale může se jednat i o důvod založení odpovědnosti státu v případě, že investice byla uskutečněna a informační a komunikační infrastruktura není v důsledku bezpečnostní expozice adekvátně funkční.

Jedná se o podobnou situaci, jako kdyby stát nejprve nalákal investory na fungující dopravní infrastrukturu – ta by ale po nějakém čase přestala být použitelnou v důsledku častého výskytu dopravních přestupků, které policie nezvládá řešit. Podobnost s dopravní infrastrukturou však z hlediska investic samozřejmě není úplná - z tohoto srovnání však každopádně vychází jako dokonale absurdní zjištění, že kybernetická bezpečnost stále není předmětem agendy investiční konkurenceschopnosti České republiky.

V porovnání s dopravní infrastrukturou je potřeba investic do kybernetické bezpečnosti z hlediska nákladovosti o několik řádů méně náročnou. Současně lze poukázat na skutečnost, že bezpečně fungující informační a komunikační infrastruktura je relevantním faktorem lokalizace přesně těch typů investic, které jsou pro Českou republiku prioritní, tj. investic do oborů s vysokou mírou přidané hodnoty. Naproti tomu investice do dopravní infrastruktury, nepoměrně ve všech směrech náročnější, zdaleka neindukují jen ten typ investičního potenciálu, o který má mít Česká republika zájem (namísto toho jde o investice do nekvalifikované mechanické práce nebo jen manipulace se zbožím typu montoven nebo logistických center). Z toho plyne, že je absurdní, pokud Česká republika investuje v režimu podpory investic do rozvoje silniční nebo železniční sítě, aniž by ve stejném režimu investovala do zajištění služeb informační společnosti nebo kybernetické bezpečnosti.

Úloha soukromoprávních iniciativ typu oborových či profesních sdružení je v tomto směru evidentní především v otázkách přenosu informací mezi podnikatelským sektorem a veřejnou mocí. K náležitému nastavení resp. zaměření příslušných investic je totiž třeba především znát reálné potřeby adresátů investiční podpory. Platí přitom, že středně velcí a velcí mezinárodní investoři zpravidla nemají zájem o podporu nebo dokonce o zajištění interních systémů bezpečnosti informací. Naopak lze podle zahraničních zkušeností předpokládat, že adekvátní zaměření investiční podpory má vést k zajištění bezpečného fungování služeb informační společnosti a poskytovat v reálném čase metodiku a asistenci pro zvládání závažných kybernetických bezpečnostních incidentů s původem mimo příslušné podnikatelské subjekty.

Jinými slovy má z hlediska investora význam, pokud hostitelský stát investuje do nástrojů k obecnému zajištění bezpečného fungování informační a komunikační infrastruktury. V tomto směru je nutno připomenout, že investory vedle provozu jejich vlastních informační struktur zajímá též dostupnost informačních a komunikačních technologií ze strany jejich obchodních partnerů a široké veřejnosti, jakož i využití veřejně dostupných služeb informační společnosti k interním organizačním procesům (práce z domova, komunikace mezi pobočkami, provoz distančních spotřebitelských terminálů apod.)

Pozitivní příklady důvěryhodné, efektivní a oboustranně výhodné vzájemné spolupráce na odborné úrovni není každopádně nutno brát jen ze zahraničí, byť je tato forma účasti průmyslových podniků na řešení odborných otázek veřejnou mocí běžná například v Německu, Spojeném Království nebo USA. Příkladem dobré praxe může být i shora zmíněný proces přípravy věcného záměru a posléze i textu paragrafového znění zákona o kybernetické bezpečnosti, kde se podařilo vést věcný dialog mezi podnikatelskou sférou a dotčenými veřejnoprávními korporacemi.

5.4 Kybernetická bezpečnost jako agenda rozvojové pomoci

V současné době existují mezi jednotlivými státy velké rozdíly co do formy a intenzity řešení problematiky národní kybernetické bezpečnosti. Nedávná studie UNODC ukázala v tomto směru nikoli překvapivé obrovské rozdíly mezi rozvojovými a rozvinutými státy zjednodušeně označované jako rozdíly mezi severem a jihem[132]. Při následném projednávání výstupů této studie v rámci expertní skupiny UNODC pro kyberkriminalitu a kybernetickou bezpečnost byly tyto rozdíly nejen evidentní ale z nebývale ostré výměny názorů vyplynula potřeba zabývat se otázkou kybernetické bezpečnosti jako integrální součástí agendy rozvojové pomoci. Důležitost dostupnosti bezpečně fungující informační a komunikační infrastruktury je totiž možno srovnat s důležitostí ostatních základních společenských funkcionalit. Vlády rozvojových států však nedisponují dostatečnými finančními ani technickými kapacitami k jejímu zajištění[133].

Z výše uvedeného plyne, že účast rozvinutých států na investicích do bezpečnosti informační a komunikační infrastruktury v rozvojových státech má být motivována a legitimována stejnými morálními důvody jako např. potravinová pomoc nebo pomoc s rozvojem základní technické nebo dopravní infrastruktury. V tomto případě však nemusí být motivace rozvinutých států pouze morální resp. sociální, ale může jít o prostý důsledek utilitaristické úvahy ekonomické resp. politické.

132 Viz dokument Srovnávací studie počítačové trestné činnosti, publ. on-line na adrese http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

133 Srov. Bande, L. C. A Case for Cybercrime Legislation in Malawi, Malawi Law Journal, roč. 5, str. 93.

Obecně platí, že je z hlediska nákladovosti výhodnější pokrývat kybernetické bezpečnostní incidenty pokud možno co nejblíže místu jejich vzniku, a to z hlediska časového i geografického. Poskytují-li pak rozvojové země z důvodu neschopnosti investovat do bezpečnostních opatření něco jako bezpečné přístavy pro vznik a vývoj kybernetických bezpečnostních incidentů, je logicky zájmem cílových států (a většinou jde naopak právě o státy rozvinuté) pokrýt příslušná bezpečnostní rizika shora popsaným způsobem.

Strategické zaměření rozvojové pomoci do sektoru kybernetické bezpečnosti může nikoli jen zprostředkovaně ale přímo pomoci řešení bezpečnostní situace nejen ve státech, kam pomoc přímo směřuje ale možná i významnějším způsobem v zemích, kde se kybernetické bezpečnostní incidenty projevují. Dárce tedy v tomto případě chrání prostřednictvím své intervence sám sebe (podobně jako např. rozvojová pomoc směřující ke zvyšování kvality života vede ke snižování nelegální migrace a omezování následných problémů ekonomických, sociálních apod.)

Rozvojová pomoc v sektoru kybernetické bezpečnosti má speciálně v případě České republiky ještě další rozměr, a to podporu tuzemského výzkumu, vývoje a průmyslu v oboru pokročilých informačních a komunikačních technologií. Česká republika se, dlužno říci i přes dosavadní absenci prakticky jakékoli veřejné resp. politické podpory, dostala na špici v oboru kybernetické bezpečnosti, ať už jde o oblast primárního výzkumu (nikoli jen v oboru ICT, ale i v oboru práva, psychologie nebo sociálních věd), experimentálního a aplikovaného vývoje či komerčních aplikací. Existuje tedy v současné době u nás řada akademických pracovišť a podnikatelských subjektů, jejichž výsledky jsou plně srovnatelné v mezinárodním (nikoli jen evropském) měřítku a mohou řešit nejen aktuální problémy naší národní kybernetické bezpečnosti, ale jsou použitelné prakticky v libovolném národním nebo nadnárodním prostředí. Zaměří-li se do toho sektoru prostředky určené na rozvojovou pomoc (tj. pokud budou české instituce díky českým rozvojovým programům řešit problémy kybernetické bezpečnosti rozvojových zemí), bude tímto způsobem možno obecně podporovat další rozvoj tohoto sektoru v České republice bez toho, aby se jednalo o zakázanou veřejnou podporu nebo jinou formu zakázaného narušování tržního prostředí.

6 MECHANISMY ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Pojem kybernetická bezpečnost je v různých zdrojích definován různě, v širším smyslu slova však pod tímto pojmem můžeme chápat souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru[134]. Při takto širokém chápání platí, že ač je gestorem problematiky kybernetické bezpečnosti v České republice Národní bezpečnostní úřad, není a ani nemůže být při zohlednění výše popsaných právních nástrojů jedinou autoritou, respektive jediným subjektem, který tuto agendu zajišťuje. Ze zákona o kybernetické bezpečnosti pro něj totiž nevyplývá plný katalog práv a povinnosti k jejímu pokrytí potřebných. To je ostatně v zásadě reflektováno i v klíčovém národním strategickém dokumentu pro oblast kybernetické bezpečnosti – Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 a k ní náležejícím akčním plánu[135] – ve kterém si Česká republika stanovila jako jeden z hlavních cílů zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti mezi jednotlivými subjekty kybernetické bezpečnosti. Do kybernetické bezpečnosti se tak v širším smyslu slova dá zahrnout rovněž oblast potírání kybernetické kriminality, zajišťování kybernetické obrany státu, ochrany kritické a významné informační infrastruktury, služeb informační společnosti, apod. Jelikož v těchto oblastech vykonávají působnost na sobě vzájemně nezávislé autority a tyto jsou rovněž regulovány různými právními normami se specifiky úpravy, je třeba se zabývat možnostmi jejich vzájemné součinnosti a limity, které pro tuto součinnost vytváří příslušný právní rámec.

---

134 Viz JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

135 Tyto dokumenty byly Vládou ČR přijaty v Usnesení vlády české republiky ze dne 23. května 2012 č. 364 o Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 a Akčním plánu opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015, a jsou dostupné online zde: https://www.govcert.cz/download/nodeid-1004/ a zde: https://www.govcert.cz/download/nodeid-973/.

Tato a následující kapitoly jsou proto zaměřeny na problematiku subjektů, které do oblasti kybernetické bezpečnosti zasahují a mechanismů součinnosti a spolupráce, které mají stanovených cílů dosáhnout. Jsou tedy zaměřeny především na Národní bezpečnostní úřad jako gestora, povinné osoby, kterým z právních předpisů vyplývají povinnosti v oblasti kybernetické bezpečnosti, orgány činné v trestním řízení vykonávající působnost v oblasti potírání kybernetické kriminality, Vojenského zpravodajství odpovědného za kybernetickou obranu státu, zpravodajských služeb, které při svojí činnosti do oblasti kybernetické bezpečnosti objektivně zasahují, či dalších orgánů vykonávajících působnost v oblasti regulace informačních a komunikačních technologií v ČR. Pozornost je rovněž věnována součinnosti soukromoprávních subjektů, které vlastní nebo spravují většinu české infrastruktury a bez jejich přispění a compliance je tedy efektivní zajištění kybernetické bezpečnosti nereálné.

Kybernetickou bezpečnosti rovněž není možné izolovaně zajišťovat na úrovni jednoho státu, kyberprostor je totiž ve své podstatě neohraničený virtuální prostor a rizika v něm vznikající nemají územně lokalizovaný charakter. Proto je třeba rovněž počítat se součinností s orgány zahraničními respektive mezinárodními. Na této úrovni se tedy následující kapitoly věnují zejména spolupráci českých subjektů kybernetické bezpečnosti s jejich zahraničními partnery, přeshraničnímu předáváni informací o kybernetických bezpečnostních incidentech a rovněž mechanismům spolupráce zprostředkovávaným mezinárodními a nadnárodními organizacemi.

6.1 Spolupráce na národní úrovni

Jak bylo zmíněno výše, základní předpokladem k efektivnímu zajištění kybernetické bezpečnosti České republiky je vytvoření efektivních mechanismů spolupráce mezi zainteresovanými subjekty jak veřejné, tak i soukromé sféry. Klíčové postavení v tomto smyslu má především Národní bezpečnostní úřad, jako gestor problematiky kybernetické bezpečnosti a rovněž jako provozovatel Národního centra kybernetické bezpečnosti. Národní centrum kybernetické bezpečnosti (NCKB)[136] sídli v Brně a je součástí

136 Vláda schválila vznik Národního centra kybernetické bezpečnosti jako součásti Národního bezpečnostního úřadu svým usnesením ze dne 19. října 2011 č. 781, které současně postavilo NBÚ do role gestora oblasti kybernetické bezpečnosti.

Národního bezpečnostního úřadu, která primárně vykonává povinnosti vyplývající ze zákona o kybernetické bezpečnosti a ze strategických vládních dokumentů. Úlohou NCKB je především koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům. Za účelem splnění těchto úkolů NCKB provozuje vládní CERT[137] České republiky (GovCERT.CZ), zajišťuje spolupráci s ostatními národními a mezinárodními CERT a CSIRT[138] týmy, připravuje bezpečnostní standardy pro jednotlivé kategorie organizací v ČR, zajišťuje osvětu a podporu vzdělávání v oblasti kybernetické bezpečnosti a realizuje výzkum a vývoj v oblasti kybernetické bezpečnosti.

V praxi tak NBÚ prostřednictvím svých organizačních celků vykonává působnost v oblastech definovaných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, dále též ZoKB). Především vede evidenci kontaktů na subjekty provozující informační a komunikační systémy kritické informační infrastruktury a významné informační systémy[139], přijímá hlášení o kybernetických bezpečnostních incidentech a podněty dalších povinných subjektů a orgánů s působností v oblasti kybernetické bezpečnosti[140]. Tyto získané informace následně vyhodnocuje a na jejich základě rozhoduje o dalším postupu, především v rámci svojí koordinační role a metodické podpory komunikuje s dalšími relevantními subjekty a povinnými osobami. Správcům kritické informační infrastruktury a významných informačních systémů může v rámci řešení kybernetického bezpečnostního incidentu rovněž ukládat provedení reaktivního nebo ochranného opatření[141]. NBÚ rovněž provádí kontrolu

137 CERT je zkratka pojmu Cybersecurity emergency response team. Národní kyberbezpečnostní tým (GovCERT.cz) na technické úrovni zajišťuje monitorování bezpečnostního stavu české infrastruktury a řeší a koordinuje postupy při výskytu kybernetických bezpečnostních incidentů. Úlohou tohoto týmu je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hraje i při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

138 Computer security incident response team – v podstatě jde o ekvivalent CERT týmu.

139 § 15 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

140 § 20 tamtéž.

141 § 11 an. tamtéž. Povinnost provést reaktivní opatření mohou mít ve stavu kybernetického nebezpečí nebo nouzového stavu rovněž poskytovatelé služeb elektronických komunikací a orgány a osoby zajišťující významnou síť. Více k charakteru reaktivních a ochranných opatření viz výše.

plnění povinností vyplývajících ze ZoKB povinnými osobami, především kontroluje soulad provedených bezpečnostních opatření s dikcí zákona[142].

Zajímavým prvkem české národní úpravy kybernetické bezpečnosti je to, že počítá s existencí dvou bezpečnostních týmů – Národního a Vládního CERTu. Vládní CERT je součástí NBÚ a Národní provozuje pod názvem CSiRT.CZ na základě veřejnoprávní smlouvy[143] uzavřené s NBÚ sdružení CZ.NIC, z.s.p.o.[144], které je správcem národní domény .cz. Model národního a vládního CERT byl zvolen k tomu, aby obě entity maximálně využily svoji institucionální povahu při ochraně národních zájmů v oblasti kybernetické bezpečnosti, přičemž je tak zajištěna možnost využití výhod postavení jak orgánu veřejné moci, tak soukromoprávního subjektu. Vládní CERT jako součást NBÚ má možnost prostřednictvím nařizovacích a sankčních institutů vykonávat státní moc vůči vitálním prvkům národní infrastruktury a Národní CERT může vykonávat funkci point of contact pro ostatní správce a subjekty provozující infrastrukturu a současně zajišťovat sběr a distribuci informací o kybernetických bezpečnostních incidentech.[145] Národní CERT tak dle ZoKB přijímá kontaktní údaje od poskytovatelů služby elektronických komunikací, subjektů zajišťující síť elektronických komunikací a od provozovatelů významných sítí, které za stavu kybernetického nebezpečí dává k dispozici NBÚ, a od provozovatelů významných sítí přijímá hlášení kybernetických bezpečnostních incidentů, která rovněž vyhodnocuje a případně koordinuje reakci a poskytuje metodickou pomoc. Informace o hlášených kybernetických bezpečnostních incidentech může předávat i NBÚ ale pouze v anonymizované podobě[146].

142 § 4 an. tamtéž. a vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Více k bezpečnostním opatřením viz výše.

143 Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti uzavřená podle § 19 an. ZoKB. Dostupná online zde: https://www.csirt.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf. Více k CSIRT.CZ viz online zde: https://www.csirt.cz.

144 Hlavními činnostmi sdružení jsou provozování registru doménových jmen.CZ, zabezpečování provozu domény nejvyšší úrovně.CZ a osvěta v oblasti doménových jmen. Více online viz http://www.nic.cz.

145 Více ke vztahu Vládního a Národního CERT viz např. Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

146 Respektive bez uvedení ohlašovatele incidentu.

Další spolupráce NBÚ a jeho organizačních složek v oblasti kybernetické bezpečnosti není v ZoKB takto detailně kodifikovaná. ZoKB toliko deklaruje, že NBÚ spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT[147], a také že NBÚ poskytuje údaje z evidence incidentů orgánům veřejné moci pro výkon jejich působnosti[148]. Spolupráce tedy buďto vyplývá z postavení a působnosti jednotlivých orgánů, nebo je založena na neformální respektive neregulované bázi.

Z orgánů veřejné moci spolupracuje NBÚ především s orgány činnými v trestním řízení. Tato spolupráce celkem je logická a nutná, neboť orgány činné v trestním řízení zajišťují mimo jiné agendu potírání kybernetické kriminality a tím hraji zásadní roli při zajišťování bezpečnosti kyberprostoru. Spolupráce je zde nutná především v případech výskytu kybernetických bezpečnostních incidentů, které mají charakter trestného činu, v rámci předávání informací důležitých pro trestní řízení či pro zajišťování kybernetické bezpečnosti, při vytváření technických, personálních a organizačních mechanismů spolupráce.

Další oblastí, ve které je spolupráce zjevně nutná je kybernetická obrana. Tu by z organizačního hlediska měl zajišťovat resort obrany, tedy Ministerstvo obrany, Armáda ČR, respektive Vojenské zpravodajství. Ač není legislativně zatím problematika kybernetické obrany dostatečně zachycena, je potřeba již nyní schémata spolupráce budovat s ohledem na zahraniční zkušenosti s prvními náznaky „kybernetické války" a s ohledem na to, že i na úrovni NATO je uvažováno o kybernetickém prostoru jako o páté válečné doméně[149].

6.2 Spolupráce na mezinárodní úrovni

Na mezinárodní úrovni je spolupráce realizována především prostřednictvím neformálních platforem. Jediným závazným právním předpisem, který ji upravuje je nedávno přijatá směrnice Evropského parlamentu a Rady (EU) č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále též „směrnice NIS").

147 § 22 odst. 2 písm. g) tamtéž.
148 § 9 odst. 3 tamtéž.
149 Viz např. online zde: http://www.nato.int/cps/en/natohq/topics_78170.htm.

Směrnice NIS ustavuje skupinu pro spolupráci, která je tvořena zástupci členských států EU, Evropské komise a agentury ENISA. Tato skupina má především sloužit k výměně informací a zkušeností jednotlivých členů s fungováním mechanismů kybernetické bezpečnosti v jednotlivých státech. Jejím cílem je rovněž sdílení best practices v oblasti zajišťování kybernetické bezpečnosti, sdílení informací o incidentech a spolupráce s povinnými osobami[150].

Druhou sítí jejíž existenci směrnice NIS zakotvuje je síť CSIRT, tedy síť vnitrostátních dohledových pracovišť kybernetické bezpečnosti. Jejími členy mají být zástupci CSIRT týmů členských států CERT-EU[151] a jako pozorovatelé Evropská komise a agentura ENISA. Tato síť má méně strategické a více praktické cíle, směřuje především ke sdílení nedůvěrných informací o kybernetických bezpečnostních incidentech, koordinaci reakce na masivnější útoky, předávání praktických zkušeností a harmonizaci postupů a mechanismů sdílení dat.

150 Viz čl. 11 směrnice.

151 CERT-EU je v podstatě dohledové pracoviště kybernetické bezpečnosti pro instituce Evropské unie. Více online viz: https://cert.europa.eu.

7 POVINNOSTI SPRÁVCŮ INFRASTRUKTUR

7.1 Skupiny povinných osob dle ZoKB

Instituty českého práva kybernetické bezpečnosti, kterým byla věnována kapitola 2 výše působí vůči skupinám povinných osob definovaných v § 3 ZoKB. Obecně jde o správce nebo provozovatele informačních a komunikačních systémů, které jsou součástí českého kybernetického prostoru[152]. Rozsah práv a povinností jednotlivých povinných osob se liší podle toho, jaký charakter a význam mají jimi provozované systémy. Proto jsou povinné osoby rozděleny do pěti skupin.

První skupinou jsou poskytovatelé služeb elektronických komunikací[153] a subjekty zajišťující síť elektronických komunikací[154], tedy subjekty vykonávající komunikační činnosti podle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích, dále též „ZEK"). Jde v zásadě především o ISP[155], kteří poskytují připojení k internetu a kteří provozují komunikační infrastrukturu pro datové přenosy. Většina těchto subjektů rovněž podléhá oznamovací povinnosti dle § 13 ZEK, a proto je jejich výčet snadno dostupný

152 Kybernetický prostor přímo ZoKB definuje v § 2 písm. a) jako „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací".

153 Za službu elektronických komunikací se dle § 2 písm. n) považuje „služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací".

154 Za síť elektronických komunikací se dle § 2 písm. h) považují „přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace"

155 Zkratka pochází z anglického Internet Service Provider, jde tedy o organizace, které vlastní připojení do internetu a poskytuje toto připojení dalším subjektům. Obvykle ještě zajišťuje rovněž činnosti s tím spojené - např. provoz mail serverů, dns serverů, routerů apod. Zdroj definice: Laboratorní encyklopedie. Laboratorní průvodce [online]. [cit. 2016-11-02]. Dostupné z: http://www.labo.cz/sl/vy07.htm.

online v evidenci[156] kterou provozuje Český telekomunikační úřad (dále též „ČTÚ"). První skupina zahrnuje největší množství subjektů, jejichž vliv na kybernetickou bezpečnost České republiky je často zanedbatelný, proto podléhá nejslabší regulaci (viz dále).

Podmnožinou první skupiny je skupina druhá, kterou tvoří orgány nebo osoby zajišťující významné sítě. Za významné sítě se přitom považují sítě elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. Jde tedy o provozovatele významných páteřních komunikačních infrastruktur[157], u kterých by narušení důvěrnosti, dostupnosti či integrity mohlo ohrozit bezpečnost ČR. Proto je pro tuto skupinu povinných osob stanoven větší rozsah povinností.

Ještě vyšším ohrožením by bylo narušení CIA triády v případě třetí a čtvrté skupiny povinných osob, kterou jsou správci informačních systémů a komunikačních systémů kritické informační infrastruktury, přičemž za kritickou informační infrastrukturu ZoKB považuje „prv[ky] nebo systém[y] prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti"[158]. Zde je úprava ZoKB navázána na jinou veřejnoprávní úpravu – konkrétně na zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon, dále též KZ). KZ totiž kritickou infrastrukturu[159] definuje a upravuje podmínky určování jednotlivých jejích prvků[160]. V rámci procesu určování prvků kritické informační infrastruktury[161] se nejprve hodnotí zda jsou dána průřezová kritéria, tedy zda by narušení CIA triády

156 Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění. Její vyhledávací rozhraní je dostupné na adrese: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.

157 Srov. např. Právní aspekty přijetí zákona o kybernetické bezpečnosti. PravoIT.cz [online]. 2015 [cit. 2016-11-02]. Dostupné z: http://www.pravoit.cz/novinka/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.

158 Viz § 2 odst. b) ZoKB.

159 Dle § 2 odst. g) KZ je kritickou infrastrukturou „prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu".

160 Prvkem kritické infrastruktury je dle § 2 odst. i) KZ „zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury".

161 Postup určování prvků kritické informační infrastruktury je přehledně popsán ve schématu dostupném zde: https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf.

příslušného informačního či komunikačního systému mohlo vést k definovaným důsledkům[162]. V druhém kroku se hodnotí zda příslušný systém spadá pod některou z kategorií specifikovaných v odvětvových kritériích – jde především o kritické prvky pevných a mobilních sítí, televizního a rozhlasového vysílání, satelitních komunikací, poštovních služeb a informačních systémů[163]. Jsou-li pro konkrétní systém kumulativně splněna průřezová i odvětvová kritéria, určí tento systém jako kritickou informační infrastrukturu NBÚ opatřením obecné povahy, jde-li o systém provozovaný soukromoprávním subjektem. Pokud je takový systém provozován organizační složkou státu, pak NBÚ navrhne Ministerstvu vnitra zařadit jej zařadit do seznamu, který bude následně předložen vládě ČR. Vláda ČR rozhodne usnesením a navrhovaný systém určí v příloze k tomuto usnesení prvkem kritické infrastruktury[164]. V rámci procesu určování kritické informační infrastruktury NBÚ s dotčenými subjekty jedná a to zpravidla ještě před samotným určením.

Pátou a poslední skupinou povinných osob dle ZoKB jsou správci významných informačních systémů, tedy informačních systémů spravovaných orgány veřejné moci, které nejsou kritickou informační infrastrukturou a u kterých by narušení bezpečnosti informací mohlo omezit nebo výrazně ohrozit výkon působnosti příslušného orgánu veřejné moci. Podobně jako je tomu v případě kritické informační infrastruktury, i významné informační se určují v rámci procedury[165], která je popsána ve vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Podle té mohou být významným informačním systémem systémy spravované orgány veřejné moci s výjimkou obcí a městských částí, které jsou v příloze vyhlášky přímo vyjmenované nebo které splňují dopadová a oblastní určující kritéria. Dopadová kritéria jsou splněná, jestliže by nefunkčnost systému

162 Tato kritéria jsou upravena v § 1 nařízení vlády č. 432/2010 Sb., takto: a) Více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin. b) Mezní hodnota hospodářské ztráty je větší než 0,5 % HDP (např. v r. 2013 = 19,4 mld. Kč). c) Omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob.

163 Odvětvová kritéria jsou upravena v příloze nařízení vlády č. 432/2010 Sb. - odvětví VI., část G.

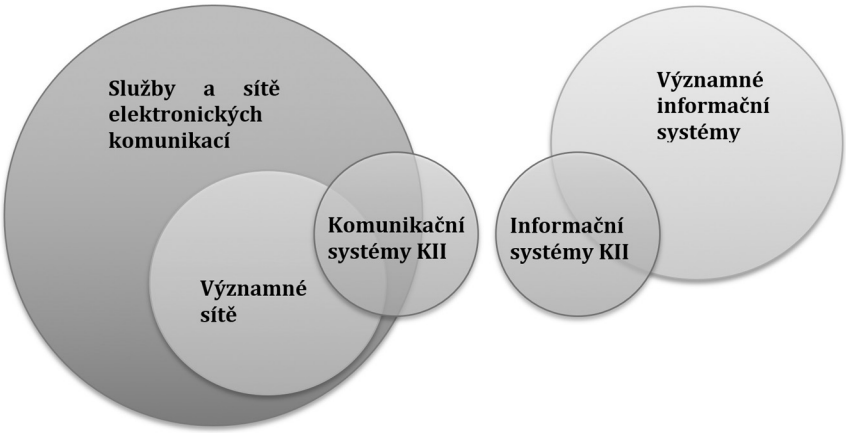
164 Podle § 2, písm. b) ZoKB se tak předmětný systém stává prvkem kritické informační infrastruktury.

165 Tuto proceduru popisuje schéma dostupné online zde: https://www.govcert.cz/download/kii-vis/container-nodeid-707/3schemavis-cz.pdf.

způsobila buď omezení výkonu působnosti příslušného správce na alespoň 3 dny[166], nebo by znamenala významné ohrožení[167], oblastní kritérium je pak splněno pokud příslušný systém vykonává některou z funkcí vyjmenovaných v příloze č. 2 k vyhlášce. Naplnění těchto kritérií posuzuje sám správce příslušného systému, který při kladném výsledku posouzení označí systém za významný interním právním aktem. NBÚ se tak do celého procesu přímo nezapojuje a poskytuje pouze podporu v podobě konzultací.

Následující schéma (obr. 1) popisuje vztahy mezi jednotlivými skupinami povinných osob, spadá-li některý informační či komunikační systém do více skupin vztahují se na něj povinnosti uložené té skupině, která jich má nejvíce. Je-li tedy například některý komunikační systém současně sítí elektronických komunikací, významnou sítí i komunikačním systémem kritické informační infrastruktury, vztahují se na jeho správce povinnosti vyplývající ze ZoKB pro správce komunikačního systému kritické informační infrastruktury.

Obr. 1 – schéma skupin povinných osob dle ZoKB



166 Srov. § 4 písm. a) vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

167 Tím že by způsobila ohrožení nebo narušení prvku kritické infrastruktury, oběti na životech s mezní hodnotou více než 10 mrtvých nebo 100 zraněných osob vyžadujících lékařské ošetření, s případnou hospitalizací s dobou delší než 24 hodin, finanční nebo materiální ztráty s mezní hodnotou více než 5% stanoveného rozpočtu orgánu veřejné moci, zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob, nebo výrazné ohrožení nebo narušení veřejného zájmu. Srov. § 4 písm. b) tamtéž.

7.2 Povinnosti povinných osob dle ZoKB

Jednotlivé skupiny povinných osob se od sebe odlišují především tím, jaké instituty ZoKB se na ně vztahují a v jakém rozsahu jim jsou tedy uloženy povinnosti.

Povinné osoby všech skupin mají povinnost oznamovat svoje kontaktní údaje a jejich změny, liší se jen subjekt kterým je poskytují. Provozovatelé služeb a sítí elektronických komunikací a správci významných sítí je poskytují národnímu CERT, zatímco ostatní skupiny Národnímu bezpečnostnímu úřadu. Institut kontaktních údajů slouží kromě jmenovité evidence povinných osob též ke komunikaci neformálních informací, oficiálních informací a závazných individuálních právních aktů vydávaných NBÚ[168]. Vzhledem k tomu, že za stavu kybernetického nebezpečí se okruh povinných osob, které mohou být povinny provádět protiopatření, rozšiřuje též o osoby, které kontaktní údaje oznamují provozovateli národního CERT, je pro tento případ rovněž upraveno předání kontaktních údajů těchto osob NBÚ.

Bezpečnostní opatření, o kterých se obecně zmiňujeme v textu výše, naproti tomu mají povinnost realizovat pouze správci systémů kritické infrastruktury a významných informačních systémů, a to navíc v různém rozsahu. Konkrétní obsah a rozsah bezpečnostních opatření a jejich dokumentace upravuje vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti[169], která je výrazně inspirovaná mezinárodními normami z oblasti bezpečnosti informací, především normami skupiny ISO 27000[170] a normami NIST[171].

168 Viz Důvodová zpráva k zákonu o kybernetické bezpečnosti.

169 Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

170 ISO/IEC 27001 je mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací. Tyto normy určuje Mezinárodní organizace pro normalizaci, známá pod zkratkou ISO (International Organization for Standardization). Více viz např. Information Security based on ISO 27001/ISO 27002 a Management Guide. 2nd ed. Zaltbommel: Van Haren Pub, 2009. ISBN 9789087535421.

171 Jde o normy publikované americkým Národním institutem pro normy a technologie (National Institute of Standards and Technology, NIST). Srovnání s ISO 27000 je dostupné např. zde: DONALDSON, Scott E., Stanley G. SIEGEL, Chris K. WILLIAMS a Abdul ASLAM. Cybersecurity Frameworks. Enterprise Cybersecurity [online]. Berkeley, CA: Apress, 2015, s. 297 [cit. 2016-11-03]. DOI: 10.1007/978-1-4302-6083-7_17. ISBN 978-1-4302-6082-0. Dostupné z: http://link.springer.com/10.1007/978-1-4302-6083-7_17.

Bezpečnostní opatření zahrnují organizační opatření, která spočívají především v úpravě vnitřních procesů a norem za účelem zajištění ochrany aktiv a řízení rizik, technická opatření umožňující fyzickou a logickou ochrany příslušného systému, řízení přístupů a logování a detekci a zpracování kybernetických bezpečnostních události a incidentů, a bezpečnostní dokumentaci sloužící k prokázání splnění stanovených povinností vůči orgánu dozoru, kterým je NBÚ. Rozsah konkrétních požadavků je u všech tří kategorií bezpečnostních opatření širší v případě provozovatelů systémů kritické informační infrastruktury.

Absenci certifikačních mechanismů diskutovanou výše vyhláška částečně zhojuje tím, že konstatuje soulad s požadavky na zavedení bezpečnostních opatření u povinných osob, které jsou příslušným akreditovaným orgánem certifikované podle ISO 27001 a vedou potřebnou evidenci[172].

Povinné osoby mají rovněž povinnost realizovat reaktivní a ochranná opatření, jejichž charakter je detailně rozebrán výše. Tuto povinnost mají správci systému kritické informační infrastruktury a významných informačních systémů. V případě vyhlášení stavu kybernetického nebezpečí[173] nebo návazně vyhlášeného nouzového stavu[174] se však povinnost provádět reaktivní opatření rozšiřuje rovněž na provozovatele služeb a sítí elektronických komunikací a významných sítí.

Další povinností, kterou ZoKB ukládá povinným osobám, je detekce a hlášení kybernetických bezpečnostních incidentů (KBI). Ta se vztahuje na správce systémů kritické informační infrastruktury, významných systémů a významných sítí. K nahlášení KBI musí dojít pomocí formuláře bezprostředně po jejich detekci, přičemž provozovatelé významných sítí je hlásí národnímu CERT, zatímco ostatní povinní NBÚ respektive vládnímu CERT, který všechny nahlášené incidenty eviduje. Hlášení KBI především umožňuje NBÚ vykonávat jeho gesci, pokud by totiž neměl informace

172 Viz § 29 Vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti.

173 Stavem kybernetického nebezpečí se dle § 21 ZoKB rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací

174 § 21 odst. 6 ZoKB.

o existujících incidentech, respektive hrozbách a vektorech útoků, mohl by jen těžko smysluplně koordinovat reakce na incidenty, informovat veřejnost prostřednictvím varování či uplatňovat reaktivní a ochranná protiopatření. Ostatně i pouhé sdílení informací v kybernetické bezpečnosti objektivně zvyšuje celkovou bezpečnost infrastruktury a snižuje náklady na její dosažení[175], proto například i často dochází k tomu, že některé soukromoprávní subjekty sdílí informace o kybernetických bezpečnostních incidentech i dobrovolně s národním CERT, nebo prostřednictvím jiných národních a mezinárodních organizací (viz dále).

Navrhovaná novela ZoKB[176] navíc navrhuje zavedení určitých doplňkových povinností. Správci a provozovatelé systémů kritické informační infrastruktury, významných systémů a systémů základní služby mají povinnost zachovávat mlčenlivost o připravovaných a přijatých bezpečnostních opatřeních. Ti z nich, kteří jsou navíc orgánem veřejné moci, budou rovněž muset si při sjednávání smlouvy s poskytovatelem cloudových služeb zajistit možnost přístupu ke svým datům uchovaným u takového poskytovatele. Nově by rovněž měla být zavedena informační povinnost správců vůči provozovatelům v případě že příslušný systém bude zařazen do kritické informační infrastruktury, či do významných systémů.

Z výše uvedeného je patrné, že jednotlivé instituty ZoKB zakládají jednotlivým skupinám povinných osob rozsah povinností korelující s významností jimi spravovaných systému pro zajištění kybernetické bezpečnosti v ČR. Vztah jednotlivých povinností a skupin povinných osob přehledně demonstruje tabulka č. 1.

175 Viz dále.
176 Viz dále v násl. podkapitole.

Tabulka č. 1 – povinné osoby a instituty ZoKB

Povinné osoby	Bezpečnostní opatření	Detekce a hlášení KBI	Reaktivní opatření	Ochranné opatření	Kontaktní údaje
Poskytovatel/ zajišťující služby a sítí el. komunikací	NE	NE	NE/ ANO*	NE	ANO – národní CERT
zajišťující významné sítě	NE	ANO – národní CERT	NE/ ANO*	NE	ANO – národní CERT
správce informačního systému KII	ANO	ANO – NBÚ	ANO	ANO	ANO - NBÚ
správce komunikačního systému KII	ANO	ANO – NBÚ	ANO	ANO	ANO - NBÚ
Správce významného informačního systému	ANO	ANO – NBÚ	ANO	ANO	ANO - NBÚ

7.3 Nové povinné osoby a jejich povinnosti v ZoKB podle směrnice NIS

Dne 8. 8. 2016 nabyla platnosti nová směrnice Evropského parlamentu a Rady (EU) č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále též „směrnice NIS"), která nově:

- zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
- ukládá členským státům povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a bezpečnostní týmy CSIRT, jejichž úkoly budou souviset s bezpečností sítí a informačních systémů;

- ukládá všem členským státům povinnost přijmout národní strategii pro bezpečnost sítí a informačních systémů;
- ustanovuje skupinu pro spolupráci, jejímž účelem je podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a budovat vzájemnou důvěru;
- ustavuje síť bezpečnostních týmů typu CSIRT, jejímž účelem je přispívat k budování důvěry mezi členskými státy a podporovat rychlou a účinnou operativní spolupráci.

Implementace této směrnice NIS do české právní úpravy, ke které musí dojít nejpozději do 9. 5. 2018, bude s největší pravděpodobností realizována transpoziční novelou ZoKB, jejíž návrh již zveřejnil NBÚ[177]. Novela se poměrně striktně drží formulací, které obsahuje samotná směrnice a počítá tak v souladu se směrnicí NIS se zahrnutím dvou nových skupin povinných osob do ZoKB - provozovatele základní služby a poskytovatele digitální služby.

Za základní služby jsou přitom považovány služby, jejichž narušení by mohlo mít významný dopad na zabezpečení klíčových společenských nebo ekonomických činností[178]. Digitálními službami jsou pak služby informační společnosti[179], které spočívají v poskytování služeb on-line tržiště[180], internetového vyhledávače nebo cloud computingu[181]. Za poskytovatele digitální služby mají být považovány všechny subjekty takovou službu poskytující, které nejsou malými podniky ani mikropodniky, zatímco provozovatele základní služby má určovat na základě navrhovaného § 22a opatřením obecné povahy NBÚ.

Kromě toho novela z důvodu praktické aplikace nové úpravy a její konzistentnosti se stávajícím režimem ZoKB zavádí navíc další skupinu povinných

177 Dostupný online zde: https://www.nbu.cz/cs/aktuality/626-navrh-na-zmenu-zakona-o-kyberneticke-bezpecnosti—-transpozice-smernice-nis/.

178 V odvětví energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, dodávek a rozvodů pitné vody, digitální infrastruktury, chemického průmyslu a veřejné správy.

179 Dle Zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

180 Které spotřebitelům umožňuje uzavírat s prodávajícím on-line kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, která využívá službu poskytovanou on-line tržištěm.

181 Jež umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet.

subjektů a to správce a provozovatele informačních systémů základní služby. Odděluje tak ve vztahu k základní službě tři subjekty – jejího poskytovatele, provozovatele jejího informačního systému a správce takového systému[182]. Ač může toto rozlišování působit poněkud nepřehledně a nesrozumitelně, má určitou logiku – s pojmem poskytovatel základní služby pracuje směrnice, pro potřeby konzistence české právní úpravy zacílení uložených povinností je však třeba oddělit poskytovatele služby a toho, kdo má pod kontrolou informační systém této služby. Takovou kontrolu může navíc vykonávat na úrovni práce s jeho funkcemi a daty správce a na úrovni technického provozování provozovatel[183]. Informační systémy základní služby má určovat opatřením obecné povahy NBÚ[184], přičemž o určení musí správce a provozovatele těchto systému informovat určený poskytovatel základní služby.

Nepřehlednost již tak komplikované právní úpravy ještě způsobuje rovněž to, že se bude poměrně často krýt kategorie významných informačních systému, informačních systémů základní služby a informačních systému kritické informační infrastruktury, přičemž na každou z nich se aplikuje zcela odlišný postup určování a rozdílné povinnosti. V návrhu pak není ani upraven vztah významného systému a systému základní služby, a tedy bude patrně platit, že správci a provozovatelé informačního systému, který bude označen za významný a současně jej NBÚ určí jako systém základní služby, budou muset plnit povinnosti ze ZoKB vyplývající pro obě skupiny správců.

Z hlediska povinností které návrh novely ZoKB novým povinným osobám ukládá lze stručně shrnout, že správci a provozovatelé systémů základní služby budou mít v podstatě stejný rozsah povinností jako a správci systémů kritické informační infrastruktury, poskytovatelé digitálních služeb pak mají povinnosti poměrně specifické v souladu se směrnicí.

Správci a provozovatelé informačních systémů základních služeb tak budou mít povinnost předávat kontaktní údaje NBÚ, realizovat bezpečnostní

182 Zde je patrná paralela k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy, který rovněž ve vztahu k informačnímu systému rozlišuje jeho provozovatele a správce. Ostatně navrhovaná novela tohoto zákona navrhuje přidání pojmu provozovatel rovněž do formulace ostatních povinných osob dle ZoKB.

183 Navrhovaná novela zákona 365/2000 Sb., která zasahuje i do ZoKB, ostatně hodlá tuto distinkci zavést i u ostatních kategorií informačních systémů.

184 K tomu bude docházet prostřednictvím procedury, ve které budou, podobě jako je tomu o významných informačních systémů, zohledněna dopadová a odvětvová kritéria.

opatření detekovat kybernetické bezpečnostní události a hlásit NBÚ incidenty a provádět reaktivní a ochranná opatření. Samotný provozovatel základní služby, který její informační systémy neprovozuje ani nespravuje, má pak mít toliko povinnost oznámit příslušnému provozovateli resp. správci zařazení systému mezi systémy základních služeb, nahlásit NBÚ že kybernetický bezpečnostní incident může ohrozit kontinuitu základní služby, a poskytnout NBÚ svoje kontaktní údaje. Dá se však očekávat, že ve většině případů bude osoba provozovatele základní služby totožná minimálně s osobou správce jejího informačního systému.

Povinnosti poskytovatele digitální služby mají v navržené úpravě částečně odlišnou povahu od ostatních povinných osob, je to dáno tím, že tato v tomto případě byly požadavky formulované ve směrnici NIS. První povinnost souvisí především s dlouhodobou tendencí EU rozšiřovat svoji jurisdikci na všechny poskytovatele online služeb kteří tyto služby nabízí na území EU[185]. Proto je vyžadováno, aby poskytovatelé digitálních služeb měli ustaveného zástupce kdekoliv na území EU. Návrh novely ZoKB tak obsahuje požadavek, aby poskytovatel digitální služby ze státu mimo EU nabízející svoje služby v ČR, měl ustaveného svého zástupce v ČR, nemá-li již takového zástupce ustaveného v jiném členském státě EU[186]. Tato úprava může být problematická zejména z toho důvodu, že na takového poskytovatele se vztahují bezpečnostní požadavky členského státu, ve kterém má svého zástupce, a ty se mohou napříč EU lišit. To by v některých případech mohlo vést ke snahám o tzv. „forum shopping"[187]. Poskytovatel digitální služby bude dále povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a informační systémy, které využívá v souvislosti se zajišťováním své služby. Tyto povinnosti se budou patrně lišit od povinnosti stanovených pro kritickou informační infrastrukturu a základní služby, neboť je toto ustanovení v zákoně oddělené a je otázka, zda bude prováděcí vyhláška po případné novele blíže takto obecně formulovaný požadavek

185 Ta je patrná především v judikatuře SDEU související s ochranou osobních údajů. Viz např. rozhodnutí SDEU ve věci Weltimmo (C-230/14) či Google Spain (C-131/12).

186 Zástupce může poskytovatel digitální služby ustavit i tak, v takovém případě se na něj vztahují povinnosti formulované v českém ZoKB, jinak na něj působí předpisy členského státu, ve kterém má zástupce. Viz § 3a novelou navrženého znění ZoKB.

187 Tedy o ustavení zástupce v tom členském státě, ve kterém je příslušná právní úprava pro poskytovatele nejvýhodnější.

specifikovat. Ačkoliv nemá podle novely poskytovatel digitální služby mít povinnost detekovat kybernetické bezpečnostní události, má povinnost hlásit kybernetické bezpečnostní incidenty s významným dopadem na poskytování jeho služeb, nebo kterékoliv základní služby.

7.4 Povinnosti vyplývající s ostatních právních předpisů

Vedle ZoKB existují v ČR i další právní normy, které ve své úpravě požadují, aby povinné osoby zajišťovaly určitou míru ochranu svých informačních infrastruktur. Tato úprava sice zpravidla zdaleka není tak konkrétní jako úprava ZoKB, přesto však k celkové kybernetické bezpečnosti českého kybernetického prostoru přispívá.

Obecné požadavky na zabezpečení informačních systémů nebo jimi spravovaných dat obsahují např. zákon 127/2005 Sb., o elektronických komunikacích (dále též „ZEK"), zákon č. 365/2000 Sb., o informačních systémech veřejné správy (dále též „ZoISVS"), zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů (dále též „ZOOÚ"), či zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále též „ZoOUI").

ZEk obsahuje především úpravu povinností poskytovatelů veřejně dostupných služeb elektronických komunikací a provozovatelů veřejných komunikačních sítí. Těm ukládá především, aby vhodnými technicko-organizačními opatřeními zajišťovali důvěrnost, bezpečnost a integritu svých infrastruktur, ochranu zpracovávaných nebo přenášených osobních údajů, provozních a lokalizačních údajů a obsahu datových přenosů. Intenzita takových opatření pak má vycházet z analýzy rizik, na základě které jsou k příslušným rizikům při zohlednění jejich závažnosti přiřazena technická respektive organizační opatření, která se mají s příslušnými riziky vypořádat. Kromě toho musí k datům a citlivým částem infrastruktury řídit přístup tak, aby se k chráněným údajům mohly dostat pouze prověřené osoby na základě příslušných opatření. Přijatá opatření pak mají být dokumentována, přičemž tato dokumentace musí být dostupná pro případnou kontrolu[188]. Ze zákona těmto povinným osobám vyplývají rovněž povinnosti informační. Předně

188 Ať již ze strany Českého telekomunikačního úřadu, či Úřadu pro ochranu osobních údajů.

musí informovat subjekty údajů, respektive Úřad pro ochranu osobních údajů, o případném ohrožení nebo narušení důvěrnosti údajů. O závažném narušení bezpečnosti a ztrátě integrity sítě, rozsahu a důvodech přerušení poskytování služby nebo odepření přístupu k ní a o přijatých opatřeních musí povinné osoby bezodkladně informovat Český telekomunikační úřad (dále též „ČTÚ"), subjekty provozující pracoviště pro příjem tísňového volání a vhodným způsobem i uživatele. ČTÚ je navíc oprávněn v případech, kdy je ohroženo nebo přerušeno nepřetržité poskytování veřejně dostupné služby elektronických komunikací rozhodnout o opatřeních nezbytných k udržení nebo obnovení tohoto poskytování[189]. Kromě toho může ČTÚ rovněž povinným osobám uložit povinnost provést bezpečnostní audit k posouzení bezpečnosti a integrity sítí a bezpečnosti služeb[190].

Velmi obecně formulovaná pak obsahuje rovněž ZoISVS, který ukládá orgánům veřejné správy, aby „[uplatňovaly] opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy"[191], které musí zohlednit rovněž v informační koncepci ve které mimo jiné stanovují sví dlouhodobé cíle s ohledem na bezpečnost spravovaných informačních systémů.

ZOOÚ po správcích či zpracovatelích osobních údajů požaduje, aby prostřednictvím vhodných technicko-organizačních opatření zabezpečili zpracovávané osobní údaje proti neoprávněnému nebo nahodilému přístupu[192], přičemž mají zohlednit především rizika neoprávněného nakládání s osobními údaji nebo prostředky jejich zpracování[193]. Tato opatření by rovněž měla umožnit určení subjektu, kterému byly osobní údaje předány, kdo a kdy je zpracoval automatizovanými prostředky, či zabránit neoprávněnému přístupu k datovým nosičům[194].

189 Viz § 62 ZEK.
190 Viz § 98 odst. 6 tamtéž.
191 § 5 b ZoISVS.
192 § 13 odst. 2 ZOOÚ.
193 § 13 odst. 3 tamtéž.
194 § 13 odst. 3 a 4 tamtéž.

Výrazně konkrétnější je ZoOUI, který požaduje zabezpečení informačních a komunikačních systémů sloužících ke zpracování utajovaných informací[195]. Poměrně konkrétní požadavky jsou pak formulovány v prováděcí Vyhlášce č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů, která vyžaduje, aby informační systémy uchovávaly auditní záznamy pro další zkoumání[196], či aby při přenosu utajované informace komunikačním kanálem byla zajištěna ochrana její důvěrnosti a integrity.

Dílčí, nebo sektorově specifická pravidla obsahují i další právní předpisy přijaté v ČR nebo na úrovni EU, rozsah této publikace však nedovoluje se jimi blíže zabývat. Zpravidla jsou však příslušné požadavky formulovány obecně a obsahují podobné požadavky jako předpisy zde zmíněné.

195 § 34 a 35 ZoOUI.

196 § 7 odst. 1 písm. c) a d) Vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Platí pro IS zpracovávající utajované informace stupně Důvěrné a vyšších.

8 SDÍLENÍ INFORMACÍ V KYBERNETICKÉ BEZPEČNOSTI[197]

Odborná veřejnost i v minulosti realizované studie[198] prokazují, že jedním z velmi efektivních a mnohdy i klíčových nástrojů využívaných pro ochranu informačních infrastruktur je sdílení informací. Je-li jeden segment propojené sítě schopen detekovat bezpečnostní hrozby a poskytnout o nich informaci ostatním segmentům, které tak mají možnost se dopředu na výskyt hrozby připravit, zvyšuje se poměrně zásadním způsobem odolnost celého prostředí. Uvědomují si to především samotní správci infrastruktur, kteří informace již nyní poměrně často dobrovolně sdílí prostřednictvím národních i mezinárodních platforem[199] Začínají si to však uvědomovat i zákonodárci, a tak začíná postupně ve světě vznikat legislativa, která ve větší či menší míře umožňuje či vyžaduje aby správci informace o hrozbách a incidentech ve svých infrastrukturách detekovali a sdíleli. Tato kapitola se proto věnu problematice právní úpravy a případných překážek se vztahem ke sběru dat pomocí analýzy datového provozu v síti a jejich následnému sdílení.

8.1 Sběr informací pomocí analýzy datového provozu

Problematika sběru informací o zranitelnostech a kybernetických bezpečnostních událostech je velmi široká. V současné době se zaměřuje především na sběr dat, která jsou komunikována uvnitř nebo vně uzavřených síťových infrastruktur. Tato podkapitola je proto zaměřena především na využití detekčních nástrojů na úrovni organizace. Tato analýza se provádí zpravidla na rozhraní mezi příslušnou sítí organizace a internetem. Analýze tak mohou podléhat nejen data organizace, ale například i data zaměstnanců

197 Části této kapitoly byly publikovány rovněž jako STUPKA, Václav. Analýza datového provozu jako prevence kybernetických bezpečnostních incidentů. Data Security Management, Praha: TATE International s.r.o., 2016, roč. 2016, č. 3, s. 44-48. ISSN 1211-8737.

198 Viz např. GORDON, Lawrence A.; LOEB, Martin P.; LUCYSHYN, William. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 2003, 22.6: 461-485., nebo LIBICKI, Martin C. Sharing Information About Threats Is Not a Cybersecurity Panacea. Technical report, RAND, 2015.

199 Například ENISA, TERENA – později GÉANT, MISP apod.

či dalších uživatelů infrastruktury – např. emailů, přenášených dat do nebo z internetu, informací o navštěvovaných webech apod.[200]. V některých případech se navíc provádí analýza i datového provozu, který je zašifrován[201]. Stále větší rozsah využívání šifrování samozřejmě zvyšuje míru důvěrnosti komunikace, v některých případech však může šifrování využívat např. malware zasílající nasbíraná data útočníkovi, nebo umožňující útočníkovi přístup do infrastruktury. Ačkoliv v případě takové komunikace uživatel oprávněně očekává větší důvěrnost, je její analýza čím dál nezbytnějším nástrojem pro zajištění kybernetické bezpečnosti.

Česká právní úprava neobsahuje konkrétní regulaci analýzy datového provozu. Naopak, relevantní úprava je spíše kusá a roztříštěná do většího množství předpisů. Jako logický první krok se při hledání aplikovatelného práva nabízí tematicky příbuzné normy, především zákon ZEK z hlediska režimu nakládání s datovou komunikací, či ZoKB, z hlediska bezpečnostních opatření.

V ZEK zákonodárce v § 89 ukládá povinným osobám bez ohledu na to, zda jde o šifrovanou nebo nešifrovanou komunikaci, zajišťovat důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů a zejména, aby nepřipustily odposlech, ukládání zpráv, nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů. Povinnými osobami jsou však ve smyslu ZEK pouze podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací[202]. Jde-li tedy pouze o datovou komunikaci v rámci vnitřní sítě jiného typu organizace, tyto povinnosti se neuplatní. Pokud by se však zamýšlená analýza týkala veřejné komunikační sítě nebo veřejně dostupné služby elektronických komunikací, mohla by být interpretována jako neoprávněný zásah do telekomunikačního tajemství.

Zákon o kybernetické bezpečnosti na tom z hlediska rozsahu subjektů, na které se vztahuje, není o moc lépe. Povinnost „v rozsahu nezbytném

200 Viz např. BARNES, Darryl T. Content Monitoring Issues Legal and Otherwise. SANS Institute. 2009.
201 Například prostřednictvím protokolu SSL.
202 Srov. § 2 písm. j) a o) ZEK.

pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření“[203] totiž ukládá toliko provozovatelům informačních a komunikačních systémů kritické infrastruktury a významných informačních systémů. Přesto však můžeme ZoKB využít alespoň jako vodítko – lze z něj totiž v obecné rovině vyčíst, co zákonodárce považuje za legitimní nástroje pro zajištění bezpečnosti infrastruktury. Bezpečnostní opatření jsou specifikována vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti (dále jen „vyhláška o KB“), přičemž její § 22 odst. 1 ukládá správcům systémů tvořících prvky kritické informační infrastruktury používat „nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.“

Veškerá zmiňovaná právní úprava formuluje bezpečnostní požadavky spíše obecně, což je vzhledem k rychlému vývoji techniky pochopitelné. Ochranu rovněž vyžaduje toliko v konkrétních případech či u konkrétních subjektů. Na druhou stranu i díky těmto legislativním požadavkům lze považovat zajištění bezpečnosti informačních a komunikačních systémů za potřebné a v zásadě i nutné. Nástroj pro analýzu datového provozu je v praxi zcela běžně používán a při zajišťování bezpečnosti infrastruktury má zcela nezastupitelnou roli[204]. Proto a i díky tomu, že je využití tohoto nástroje předpokládáno prováděcím předpisem ZoKB, lze jej považovat za vhodný prostředek ochrany informační a komunikační infrastruktury. Jsou-li pak identifikována dostatečná rizika, mohla by být v určitých případech ospravedlněna rovněž analýza provozu šifrovaného.

Skoro by se tak chtělo říci, že jestliže není provozovatel infrastruktury povinnou osobou podle ZEK, může podle zásady „je povoleno, co není výslovně zakázáno“ bez obav jakákoliv data přenášená z nebo do svojí vnitřní sítě jakýmkoliv způsobem podrobovat analýze a případně dešifrovat. Tak tomu ale samozřejmě není. Je totiž nutné rovněž hledět na základní práva uživatelů dané infrastruktury. V případě vnitřní sítě organizace jimi budou především zaměstnanci, případně jiné osoby, kterým je umožněno se do příslušné

203 § 4 odst. 2 ZKB.

204 Srov. CECIL, Alisha. *A summary of network traffic monitoring and analysis techniques*. Computer Systems Analysis, 2006, 4-7.

sítě připojovat. Má-li být jimi realizovaná komunikace podrobena analýze, je nutné zohlednit možné občanskoprávní, pracovněprávní či správněprávní podmínky takového zásahu do soukromí a důsledky, které mohou eventuálně nastat.

Dle § 81 zákona č. 89/2012 Sb., občanský zákoník (dále jen „OZ"), je chráněna osobnost člověka včetně všech jeho přirozených práv, přičemž ochrany požívají zejména mezi jinými soukromí člověka a jeho projevy osobní povahy jako např. „písemná vyjádření a písemnosti osobní povahy […] bez ohledu na osobu původce této písemnosti."[205] Podstatou práva na ochranu soukromí je „především možnost vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti osobního soukromí člověka zpřístupněny jiným subjektům."[206] V rámci ochrany soukromí pak „zvláštní ochrany požívají rovněž informace v soukromé korespondenci člověka či údaje o komunikačním provozu."[207] Analýza datového provozu se pochopitelně týká i komunikace osob využívajících příslušnou síťovou infrastrukturu, je tak při její realizaci do určité míry zasahováno do jejich autonomie rozhodování zda a komu komunikovaný obsah zpřístupní a tím pádem dochází k zásahu do soukromí porušením ochrany projevů osobnostní povahy.

OZ však pro tyto případy stanoví výjimku, v rámci které je možné zasahovat do ochrany soukromí, je-li to nutné „k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob"[208]. Této výjimky však „nesmí být využit[o] nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka."[209] Lze tedy konstatovat, že z hlediska OZ k analýze datového provozu může provozovatel infrastruktury přistoupit, ale musí při ní prokazatelně přiměřeně šetřit práva uživatelů, přičemž zákonná úprava celkem pochopitelně nestanoví, jak konkrétně správně postupovat.

Kromě obecné úpravy OZ cílí na ochranu soukromí rovněž zákon č. 101/2000 Sb., o ochraně osobních údajů (dále též „ZOOÚ"), který

205 LAVICKÝ, P. a kol.: *Občanský zákoník I.* Obecná část (§ 1−654). Komentář. 1. vydání, Praha: C. H. Beck, 2014. s. 397.
206 Tamtéž s. 445.
207 Tamtéž s. 516.
208 § 88 odst. 1. OZ
209 § 90 OZ.

upravuje podmínky a limity zpracování osobních údajů. Za osobní údaje ZOOÚ považuje „[jakoukoliv] informac[i] týkající se určeného nebo určitelného subjektu údajů […]“[210], zpracování pak je „jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji […]“[211]. Díky takto širokým definicím se ZOOÚ na analýzu datového provozu jednoznačně vztahuje[212], neboť předmětné datové přenosy osobní údaje obsahují[213], nebo alespoň mohou obsahovat. Dle dikce zákona může takové zpracování správce provádět pouze svědčí-li mu některý ze zákonných titulů uvedených v § 5 odst. 2 ZOOÚ. Základním titulem je souhlas subjektu údajů, nicméně bezpečnostní analýzu datového provozu lze rovněž provádět, je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Takové zpracování osobních údajů však nesmí být v rozporu s právem subjektů údajů na ochranu jeho soukromého a osobního života.[214] Úpravu ZOOÚ má do budoucna nahradit Obecné nařízení o ochraně osobních údajů[215]. To se z hlediska právních důvodů zpracování osobních údajů či zásad směřujících k jejich ochraně od současné právní úpravy příliš neliší. Má však širší záběr – v nařízení se jako

210 § 4 písm. a) ZOOÚ. Celá zákonná definice zní: „osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,“

211 § 4 písm. e) ZOOÚ. Celá zákonná definice zní: zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

212 Toto stanovisko podporuje např. i text odst. 26 preambule směrnice č. 2002/58/ES, směrnice o soukromí a elektronických komunikacích, či Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009.

213 Respektive provozovatel síťové infrastruktury nemůže vyloučit, že součástí datových přenosů budou. I když se budou v datovém přenosu objevovat osobní údaje sporadicky, není-li možné tyto z analýzy spolehlivě vyloučit, je třeba s celým obsahem takového nakládat jako by osobní údaje obsahoval. Více viz např. KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Vyd. 1. Praha: C. H. Beck, 2012. 516 s. Beckova edice komentované zákony. ISBN 9788071792260.

214 § 5 odst. 2 písm. e) ZOOÚ.

215 Nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále též jako „GDPR“).

o osobním údaji výslovně hovoří např. i o IP adrese či cookies[216], zavádí více povinností pro správce – nově např. bude muset správce vést detailní záznamy o provedeném zpracování údajů[217] či implementovat principy „data protection by design and by default"[218], a stanovuje výrazně citelnější sankce – ve výši až 20 mil. EUR nebo až 4 % celosvětového obratu správce.

Lze tedy shrnout, že i v souladu s právní úpravou ochrany osobních údajů lze analýzu datového provozu teoreticky provádět; ani tentokrát se však nedozvídáme jak v praxi dosáhnout obecně formulovaných požadavků na ochranu soukromí, respektive jak konkrétně správně postupovat.

Aby toho nebylo málo, musíme zohlednit rovněž ochranu soukromí zaměstnanců, obsaženou v zákoně č. 262/2006 Sb., zákoníku práce (dále též „ZP"). Jeho § 316 odst. 2 zakazuje zaměstnavateli „bez závažného důvodu […] narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, [nebo] kontrole elektronické pošty […]." Přestože je takové sledování zaměstnanců předpokládáno za účelem kontroly dodržování zákazu využití pracovních prostředků pro osobní potřebu, je tato formulace natolik široká, že může pokrývat sledování datového provozu i za jinými účely. Proto se domnívám, že bude-li zaměstnavatel sledovat datové přenosy z počítače zaměstnance za účelem prevence kybernetických bezpečnostních incidentů, je nutné k § 316 odst. 2 a 3 minimálně přihlédnout.

Z výše zmíněného poměrně jednoznačně vyplývá, že analýzu datového provozu za účelem prevence, detekce a analýzy kybernetických bezpečnostních incidentů provádět lze, nicméně pouze za podmínek a v souladu s příslušnými právními předpisy. Tyto podmínky jsou však formulovány velice obecně a je proto nutné se jimi na teoretické úrovni zabývat.

Prvním a základním předpokladem provádění analýzy datového provozu je vyvážení práv provozovatele infrastruktury na zajištění její bezpečnosti a práv

216 V recitálu č. 26 GDPR.

217 Čl. 30 tamtéž.

218 Tyto principy vyžadují, aby již při designování postupu zpracování osobních údajů byl brán ohled na jejich ochranu a aby bylo prostřednictvím organizačních a technických opatření zajištěno, že budou zpracovávány jen a pouze ty osobní údaje, které je nutné zpracovat za účelem dosažení definovaného účelu. Zakotveno v čl. 25 GDPR.

osob infrastrukturu využívajících na ochranu soukromí. K tomu lze využít nástroje označovaného za test proporcionality, který vychází z kontinuální judikatury Ústavního soudu[219] a který zohledňuje kritérium vhodnosti, potřebnosti a poměřování. Analýza datového provozu je jednoznačně vhodným nástrojem k zajištění bezpečnosti informační infrastruktury[220], současně jde v mnoha případech o nástroj potřebný v tom smyslu, že jiným, do práva na soukromí nezasahujícím způsobem, bezpečnost ekvivalentně zajistit nelze[221].

Problematické je především hledisko poměřování, v rámci kterého je třeba hledat takové řešení, kdy závažnost požadavku na zajištění bezpečnosti je tak vysoká, že odůvodňuje příslušnou míru zásahu do práva na soukromí. Je tedy třeba zvolit technická, organizační a právní mechanismy, které zásah do tohoto práva dostatečně zmírní[222].

V první řadě by měla být provedena analýza rizik, která by identifikovala významnost jednotlivých součástí infrastruktury, jejích zranitelnosti a míru a rozsah, ve kterých by mělo k analýze docházet. To umožní zvolit technologii zajišťující dosažení cílů při minimálním zásahu do práv uživatelů. Tento postup je ostatně vyžadován či doporučován i např. v prováděcích předpisech ZoKB[223], v normách v oblasti informační bezpečnosti[224] či v odborné literatuře[225]. Analýza rizik je rovněž součástí Posouzení vlivu na ochranu osobních

219 Do našeho právního řádu byl tento test zaveden kontinuální řadou rozhodnutí Ústavního soudu, je formulován např. v rozhodnuti ze dne 12. 10. 1994, sp.zn. Pl. ÚS 4/94 nebo ze dne 21. 3. 2002, sp.zn. III. ÚS 256/01. K pojmu a metodě viz též např. viz Alexy, R. *On the Structure of Legal Principles*. Ratio Iuris. 2000, roč. 13, č. 3, str. 1 a násl. nebo Holländer, P. *Filosofie práva*. Plzeň: Aleš Čenek, 2006, str. 158 a násl.

220 Srov. např. MINAŘÍK, Pavel. *Pokročilá analýza provozu datových sítí*. IT Systems [online]. 2015, 2015(1) [cit. 2016-07-08]. Dostupné z: https://www.systemonline.cz/it-security/pokrocila-analyza-provozu-datovych-siti.htm

221 Tomu napovídá i zahrnutí tohoto nástroje v požadavcích na bezpečnostní opatření v zákoně o kybernetické bezpečnosti.

222 Což ostatně do určité míry vyžaduje i zákon o ochraně osobních údajů v § 13 odst. 2 až 4.

223 Viz především § 3 a 4 Vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

224 Např. skupina norem ČSN ISO/IEC 27000.

225 Viz např. DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. *Řízení bezpečnosti informací*. 2. vydání. Praha: Professional publishing, 2011, 240 str., ISBN 978-80-7431-050-8., nebo ONDRÁK, V., SEDLÁK, P., MAZÁLEK, V. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

údajů, jehož zpracování bude vyžadovat GDPR v případech rozsáhlého zpracování osobních údajů nebo monitorování veřejně přístupných prostorů[226].

Kupříkladu dešifrování a analýzu SSL provozu je vhodné provádět jen v kritických systémech, kde je malá pravděpodobnost výskytu soukromé komunikace. Je rovněž vhodné využívat v co nejširší míře automatizované analýzy založené na metadatech a v co nejmenší míře naopak analyzovat obsah. V některých případech bude pro změnu vhodné síť logicky segmentovat a v jednotlivých částech podle jejich povahy provádět různé metody analýzy[227]. Možné je rovněž využívání různých whitelistů a blacklistů[228] které určí jaká komunikace má a nemá podléhat analýze. Jde prostě o to využít vhodné technické prostředky ke zmírnění zásahu do soukromí.

Dále je vhodné provést organizační opatření, a to taková, která zajistí, aby analytická data, která mohou obsahovat soukromá data, byla zabezpečena proti neoprávněnému a nahodilému přístupu[229]. Jde především o volbu vhodného a zabezpečeného úložiště takových dat a o řízení přístupu k němu. S těmito daty by pak v souladu s příslušnými vnitřními instrukcemi měli nakládat pouze vymezení a prověření zaměstnanci se zákonnou i smluvní povinností mlčenlivosti[230].

Vhodným nástrojem je rovněž informování uživatelů infrastruktury o možnosti a rozsahu provádění analýz[231]. Nejenže se tím zvýší obecně jejích legitimita, ale rovněž se tak sníží míra, ve které je uživateli důvodně očekáváno soukromí realizované komunikace[232]. Vhodným nástrojem zde může být vnitřní instrukce v podobě podnikových směrnic či podmínek využívání infrastruktury.

226 Srov. čl. 35 GDPR.

227 Např. komunikace wifi routeru v zasedací místnosti, ve které se mohou návštěvy připojovat k internetu, může být logicky oddělena od ostatních datových přenosů a vyloučena z analýzy.

228 Např. do whitelistu je vhodné zahrnout servery internetového bankovnictví, u kterých lze presumovat bezpečnosti a komunikace s nimi nemusí podléhat analýze, a do blacklistu například sociální sítě, které riziko představuje a zpravidla pro výkon práce či návštěvníky nejsou potřebné.

229 Tento požadavek výslovně obsahuje i Zákon o ochraně osobních údajů. Srov. Viz § 5 odst. 1 ZOOÚ.

230 Tu vyžaduje rovněž ZOOÚ.

231 Do určité míry je tento požadavek formulován v případě zaměstnanců v zákoníku práce. Viz např. BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce.* Komentář. 2. vydání. Praha: C. H. Beck, 2015. s. 1243.

232 K očekávání zaměstnance viz Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009.

Lze rovněž doporučit, aby využití těchto i jiných použitých technických a organizačních prostředků bylo vhodně dokumentováno. Nejenže je taková dokumentace užitečným nástrojem při prokazování compliance, bude navíc požadována v rámci nové právní úpravy v GDPR.

Ačkoliv je analýza datového provozu zcela běžně prováděnou technikou zajišťující zabezpečení infrastruktur organizace, zpravidla se příliš nezamýšlíme nad jejími právními implikacemi. Podmínky využívání těchto bezpečnostních technologií a přesné postupy, které by měli příslušní provozovatelé infrastruktur realizovat, se patrně budou odvíjet od konkrétních podmínek konkrétní infrastruktury, od její povahy, od povahy dat, které zpracovává a případně o charakteru jejích uživatelů. Je tedy třeba zvážit příslušnou právní úpravou, která by při implementaci a využívání nástrojů pro analýzu datového provozu měla být zohledněna. Na základě příslušné legislativy pak lze formulovat související právní problémy, kterými se musí příslušní provozovatelé zabývat, a navrhnout jejich možná právní, organizační a technická řešení.

8.2 Dobrovolné sdílení informací v kybernetické bezpečnosti

Je obecně uznáváno, že jednou z vhodných metod podpory zabezpečení informačních infrastruktur na úrovni organizací i celého prostředí sdílení informací o kybernetických bezpečnostních událostech a incidentech.[233] Kromě toho je rovněž považováno za vhodné sdílet informace související s předcházením, detekováním a záplatováním bezpečnostních zranitelností, neboť tak organizace mohou předejít možným škodám, které utrpěly nebo kterým zamezily jiné organizace.[234] Současné díky dostupnosti takových informací mohou organizace při výskytu podobného útoku efektivněji reagovat a využít vhodných prostředků k obraně.

233 Srov. GROUP, Tom. Why Cybersecurity Information Sharing Is Important. RSA Conference [online]. 2016 [cit. 2016-11-06]. Dostupné z: https://www.rsaconference.com/blogs/why-cybersecurity-information-sharing-is-important.

234 K tomu viz např. GORDON, Lawrence A., Martin P. LOEB a William LUCYSHYN. Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy. 2003, 22(6), 39.

Podle studie organizace ENISA[235] existují tři typy přístupu ke sdílení informací v oblasti kybernetické bezpečnosti. Prvním je tradiční autoritativní regulace, druhým alternativní režim regulace jako seberegulace či spolupráce a třetím specifické přístupy ke sdílení informaci prostřednictvím informačních a vzdělávacích schémat.

Studie[236] rovněž ukazují, že ačkoliv roste množství států, které prostřednictvím legislativy ukládají správcům povinnosti směřující ke sdílení informaci, zůstávají mechanismy pro dobrovolné sdílení převažujícím modelem ve většině moderních zemí. Příslušná legislativa se totiž zaměřuje především na sdílení dílčích informací o kybernetických bezpečnostních incidentech a realizovaných úspěšných útocích, navíc je z mezinárodního hlediska nekonsistentní jelikož různé státy mají při tvorbě regulace různé přístupy.

Ani dobrovolné sdílení však není ani zdaleka bezproblémové. Důvodem je především neochota sdílet údaje projevující se především v některých odvětvích, která je často odůvodněná na jedné straně obavou organizací z toho, že ztratí kredibilitu když se zveřejní informace o jejich zranitelnosti či realizovaném útoku, a na druhé straně i obavou ze striktní právní úpravy ochrany osobních údajů a z ní vyplývajícího rizika vzniku právní odpovědnosti. Vedle toho je do určité míry problémem rovněž nekoordinovanost sdílecích mechanismů v rámci jednotlivých platforem, a nemožnost sankcionování těch členů platforem, kteří informace ostatních ochotně využívají ale vlastní z výše uvedených nebo jiných důvodů neposkytují.

V České republice je díky existenci ZoKB a díky poměrně úspěšným aktivitám NBÚ a národního CERT v posledních letech v této oblasti patrný značný posun. ZoKB sdílení určitých údajů přímo požaduje[237], zatímco pro jiné vytváří alespoň právní rámec a platformu. Údaje nasbírané od povinných osob, které hlásí kybernetické bezpečnostní incidenty, může NBÚ poskytovat národnímu CERT a jiným subjektům působícím v oblasti kybernetické bezpečnosti, je-li to potřeba k zajištění ochrany kybernetického prostoru[238],

235 Viz EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. 2015. ISBN 978-92-9204-131-1.
236 Tamtéž.
237 Viz výše.
238 § 9 odst. 4 ZoKB

národní CERT pak může jemu nahlášené údaje poskytovat v anonymizované podobě NBÚ[239]. Národní CERT, který je osobou soukromého práva a vykonává svou funkci na základě veřejnoprávní smlouvy uzavřené s NBÚ, může být pak vhodným partnerem a platformou i ke sdílení informací o incidentech, které poskytují nejen povinné osoby, ale i dobrovolně zapojené subjekty. Národní CERT tak plní vlastně roli koordinátora, který sbírá údaje, koordinuje reakci a poskytuje tyto údaje adresně tam, kde jsou potřeba. Národní CERT současně poskytuje pomoc ostatním organizacím v případě, že chtějí zřídit vlastní bezpečnostní tým, nebo jej zapojit do mezinárodní infrastruktury Trusted Introducer[240].

Národní CERT však v současné době neposkytuje platformu, která by umožňovala automatizované sdílení širšího spektra informací v oblasti kybernetické bezpečnosti. Klíčová totiž často nejsou pouze hlášení kybernetických bezpečnostních incidentů, ale například i událostí nebo známých zranitelností. Za tím účelem však v ČR i na mezinárodní úrovni platformy existují. V ČR je v této oblasti asi nejaktivnější akademické sdružení CESNET[241], který provozuje detekční platformu Mentat[242], sdílecí platformu Warden[243] a v současné době v rámci výzkumného projektu připravuje nástavbu pro analýzu bezpečnostních dat Sabu[244]. Jde o výsledky výzkumných projektů, které jsou využívány některými bezpečnostními týmy v ČR, a slouží jako proof of concept.

Jedním ze zásadních problémů při sdílení dat o bezpečnostních incidentech, událostech, zranitelnostech a anomáliích je, že pro něj v obecné rovině neexistuje právní rámec. Hlavní překážku pak tvoří především ochrana soukromí a osobních údajů. Jak bylo řečeno výše, identifikátory používané k adresování komunikace při datových přenosech mohou být považovány za osobní údaje[245]. A to i přesto, že SDEU ve svém nedávném rozhodnutí

239 § 17 odst. 2 písm. g) tamtéž.
240 Viz online: https://www.trusted-introducer.org/.
241 CESNET je zájmové sdružení právnických osob, které sdružuje akademické instituce v ČR. Více online zde: http://www.cesnet.cz.
242 Více online viz: https://mentat.cesnet.cz/.
243 Více online viz: https://warden.cesnet.cz/.
244 Více online viz: https://sabu.cesnet.cz/.
245 Více k tomuto viz např. HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. Revue pro právo a technologie. 2015, 6(12), 22. ISSN 1805-2797.

částečně ustoupil z dosavadního striktně objektivního chápání osobního údaje, když konstatoval, že IP adresa nemusí být ve vztahu ke konkrétnímu správci považována za osobní údaj jestliže tento nemá rozumně použitelné prostředky pro její identifikaci k určitému subjektu údajů[246]. Správci, kteří chtějí sdílet bezpečnostní data tak musí fungovat v režimu právní úpravy ochrany osobních údajů a především pak hledat právní titul pro jejich zpracovávání a sdílení. Ačkoliv v souladu se ZOOÚ poskytuje Úřad pro ochranu osobních údajů konzultace[247], jen velmi zřídka je ochoten předem závazně konstatovat soulad či nesoulad určitého postupu nebo výkladu s požadavky zákona. Správci tak často riskují, že se sdílením i v dobré víře dostanou do rozporu se zákonnými požadavky a budou sankcionováni. Určité řešení by do budoucna mohlo nabízet nařízení GDPR, které vytváří nové instituty kodexů chování a osvědčení[248]. Kodexy chování by měly popisovat postupy při určitém druhu zpracovávání osobních údajů. Měla by vypracovávat zájmová sdružení správců určité kategorie a předkládat je dozorovým orgánům ke schválení. Dozorové orgány by měly při schvalování posoudit a následně monitorovat soulad formulovaných postupů s požadavky ochrany osobních údajů. Pokud by pak konkrétní správce podle příslušného kodexu postupoval, měl by určitou záruku, že jedná legálně. Podobně by mělo fungovat osvědčení, které by se mělo vydávat konkrétnímu správci či zpracovateli po auditu jeho způsobu nakládání s osobními údaji, který by měl provádět akreditovaný subjekt. Jak budou tyto instituty v praxi fungovat však v současné době není jasné a lze jen těžko spekulovat, do jaké míry budou využitelné pro komunitní sdílení dat v kybernetické bezpečnosti.

8.3 Exkurs – srovnání přístupu v ZoKB s úpravou sdílení informaci v USA

V USA je sdílení informací v kybernetické bezpečnosti upraveno v navrhovaných předpisech takzvaného kyberbezpečnostního balíku. Ten obsahuje celkem pět návrhů zákonů které mají za cíl buď umožnit sdílení

246 Viz rozhodnutí ve věci Breyer (C-582/14).
247 § 29 odst. 1 písm. a) ZOOÚ.
248 Čl. 40 a 42 GDPR.

informací o kybernetických bezpečnostních incidentech (CISPA, CISA[249], CTSA[250]), nebo nastavit procedury pro realizaci takového sdílení (PCNA[251], NCPAA[252])[253]. CISPA, CISA a CTSA jsou normy umožňující soukromým společnostem sbírat a uchovávat data o kybernetických incidentech a tato data sdílet s federální vládou. Mechanismus sdílení i rozsah sbíraných a sdílených dat se v jednotlivých předpisech liší jen v detailech, menší rozdíly jsou rovněž v mechanismu ochrany soukromí.

Tyto normy prošly ve srovnání s ZoKB výrazně komplikovanější legislativní procedurou, čemuž se však v USA nelze moc divit. Z části v tomto hraje roli boj politické reprezentace, ale hlavním důvodem je to, že občanští aktivisté a neziskové organizace jsou po aféře Snowden, která odhalila praktiky amerických úřadů v oblasti kybernetické bezpečnosti a kriminality, velmi obezřetní když jakýmkoliv způsobem hrozí, že budou rozšířeny možnosti zásahu do ochrany soukromí chráněného dodatky ústavy USA, a to jak ze strany státních orgánů, tak ze strany soukromých společností. Jediným úspěšným návrhem úpravy sdílení z balíku tak je Cybersecurity information sharing act (CISA), který prošel demokratickým Senátem úspěšněji, jako přílepek k zákonu o konsolidovaných prostředcích, a byl podepsán prezidentem Obamou v prosinci 2015.

Jak CISA, tak i ZoKB jsou předpisy, které směřují k zajištění kybernetické bezpečnosti prostřednictvím sdílení informací. Každý předpis však volí poněkud odlišný přístup k tomu, jak má sdílení informací vypadat a jak má být koordinováno. Zákonodárce v CISA předpokládá, že budou soukromé společnosti využívat detekční nástroje a poskytovat informace o kybernetických incidentech a hrozbách dobrovolně, navrhovaná úprava dokonce zapovídá

249 Viz Cybersecurity Information Sharing Act of 2015 - S.754, 114th Congress. [online]. [cit. 2016-01-02]. Dostupné z: https://www.congress.gov/bill/114th-congress/senate-bill/754/.

250 Viz Cyber Threat Sharing Act of 2015 - S.456, 114th Congress. [online]. [cit. 2016-01-04]. Dostupné z: https://www.congress.gov/bill/114th-congress/senate-bill/456.

251 Viz Protecting Cyber Networks Act - H.R. 1560, 114th Congress. [online]. [cit. 2016-01-04]. Dostupné z: https://www.congress.gov/bill/114th-congress/house-bill/1560.

252 Viz National Cybersecurity Protection Advancement Act of 2015 - H.R. 1731, 114th Congress. [online]. [cit. 2016-01-04]. Dostupné z: https://www.congress.gov/bill/114th-congress/house-bill/1731.

253 GELLER, Eric. Your complete guide to the 5 cybersecurity bills in Congress. The Daily Dot [online]. 2015 [cit. 2016-01-2]. Dostupné z: http://www.dailydot.com/politics/congress-cybersecurity-threat-sharing-bills-explained-cisa-cispa-pcna/

státní moci uložit povinnost poskytnutí takových informací soukromoprávním subjektům. CISPA tak vytváří právní a procedurální rámec pro dobrovolné sdílení, především vylučuje odpovědnost soukromoprávních subjektů za sběr, využívání a sdílení informací za účelem zajištění kybernetické bezpečnosti v dobré víře. Český ZoKB naopak přímo předepisuje vyjmenovaným povinným osobám využívat detekčních nástrojů pro identifikaci kybernetických bezpečnostních incidentů a rovněž povinnost hlásit bezpečnostní incidenty, které se v jejich sítích vyskytnou. Úpravu sdílení dalších informací či výslovné vyloučení odpovědnosti povinných subjektů však neobsahuje.

Rovněž rozsah informací, které mají být na základě diskutovaných předpisů sbírány a sdíleny se liší. CISA předpokládá sdílení informací o kybernetických hrozbách (cyber threat information), tedy o zranitelnostech systémů nebo sítí, o hrozbě pro zajištění CIA triády systémů nebo sítí nebo informací v nich zpracovávaných, o snahách o znedostupnění nebo poškození systémů či sítí a o snahách o neoprávněný přístup do systémů nebo sítí. Tyto informace pak mohou sdílet společnosti zajišťující bezpečnostní služby dodavatelsky se souhlasem svých odběratelů, nebo subjekty, které si kybernetickou bezpečnost zajišťují ve vlastní režii. V souladu se ZoKB povinné osoby sbírají různé informace o fungování příslušných systémů a sítí prostřednictvím nástrojů pro ochranu integrity komunikačních systémů, pro ověřování identity uživatelů a řízení přístupů, pro ochranu před škodlivým kódem, pro zaznamenávání činností systémů a uživatelů a pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí. Tyto nástroje mají povinnost využívat jen některé povinné osoby v závislosti na charakteru provozovaných systémů, ostatní je však pochopitelně v různé míře využívají dobrovolně. Co se týče sdílení těchto informací, jediné, co musí povinné osoby poskytovat je hlášení kybernetických bezpečnostních incidentů, a to prostřednictvím formuláře, který je součástí prováděcí vyhlášky k ZoKB. Hlášení obsahuje pouze základní informace o incidentu – kontaktní údaje správce, informace o době, kategorii a typu incidentu, průběh incidentu a odhad rozsahu škod. Lze předpokládat, že budou správci na dobrovolné bázi sdílet s komunitou, jinými správci, nebo i se státními orgány i další informace a to v rozsahu, v jakém jim to právo umožňuje. Konkrétní vyloučení odpovědnosti při takovém sdílení však na rozdíl od CISA ZoKB neobsahuje.

V souladu s CISA mohou být informace o kybernetických hrozbách sdíleny s dvěma vládními subjekty určenými prezidentem. V rámci Ministerstva pro vnitřní bezpečnost (Department of Homeland Security) má být určen subjekt, který bude sbírat informace o kybernetických bezpečnostních hrozbách, a v rámci Ministerstva spravedlnosti (Department of Justice) bude určen subjekt, který bude přijímat informace o kybernetických hrozbách souvisejících s kybernetickou kriminalitou[254]. Takto získané informace pak mohou být využity pouze pro zajišťování kybernetické bezpečnosti, pro vyšetřování kybernetické kriminality a pro stíhání šíření dětské pornografie. Tyto účely jsou však popsány velmi obecně a není ani omezen způsob či metoda využití získaných informací, mohou proto teoreticky být prohledávány, či dále sdíleny se soukromoprávními či veřejnoprávními subjekty.

V souladu se ZoKB jsou informace o bezpečnostních incidentech také sdíleny se dvěma subjekty, ale celý mechanismus funguje jinak. Zákon počítá s existencí dvou celostátních týmů CERT. Prvním je národní CERT, který je provozován soukromoprávním subjektem (viz výše). Ten přijímá povinná hlášení kybernetických bezpečnostních incidentů od správců významných sítí, a od ostatních správců může získávat další dobrovolně poskytnuté informace. Ty může využívat volně v rámci svojí činnosti při zajišťování kybernetické bezpečnosti a i sdílet v rámci vytvořené komunity. To vše pochopitelně v souladu se zákonnými limity. Jelikož jde o osobu soukromého právo, může činit vše co není zákonem zakázáno. Druhým je CERT vládní jako součást NBÚ, který sbírá povinná hlášení od správců kritické infrastruktury a provozovatelů významných informačních systémů a dále přijímá informace od národního CERTu, či dobrovolně poskytnuté informace od vnitrostátních i zahraničních subjektů. Tyto informace může NBÚ využívat pro výkon svých povinností souvisejících se zajišťování kybernetické bezpečnosti podle zákona, a může je rovněž sdílet s ostatními orgány veřejné moci v rámci výkonu jejich působnosti, s národním CERTem a zahraničními i českými subjekty působícími v oblasti kybernetické bezpečnosti.

254 Ta je chápání spíše v užším smyslu slova, zahrnuje tedy především pokusy o napadení systémů, neoprávněný přístup, neoprávněné získávání informací, a podvody související s počítači.

Nutno dodat, že zatímco v ČR jsou informace poskytnuté v souladu se ZoKB chráněny především mlčenlivostí zaměstnanců NBÚ, obecně ochranou osobnosti a osobních údajů a využitelností informací pro omezené účely, ochrana soukromí je v úpravě CISA výrazně konkrétnější. Výslovně jsou zmíněny kategorie informací, které nesmí státní orgány využít, je stanoveno, že mohou získané informace využívat toliko k vyjmenovaným účelům. Navíc musí dotčené orgány vypracovávat pravidelné reporty o rozsahu a způsobech využívání informací a o jejich ochraně soukromí při nakládání s nimi. Specifická část navrhované americké legislativy je rovněž věnována sdílení zpravodajských informací od zpravodajských služeb směrem k soukromým subjektům.

Je tedy patrné, že ZoKB, který prošel legislativním procesem poměrně lehce, striktně předepisuje jasně definované a poměrně široké povinnosti které musí povinné osoby aplikovat a rovněž předepisuje určitý minimální rozsah informací o bezpečnostních incidentech které musí závazně státnímu orgánu poskytnout, v USA bylo naopak velmi komplikované i prosazení CISA, který téměř žádné povinnosti neukládá, a toliko umožňuje soukromým subjektům bez obav sdílet informace, které jsou důležité pro zajištění kybernetické bezpečnosti. Zatímco v případě ZoKB obecné formulace nečinily zásadní překážku jeho přijetí, v případě CISA jde o velmi diskutovaný problém, na který všichni občanští aktivisté upozorňují. Stigma z kauzy Snowden má stále velký vliv a ochránci soukromí se poměrně pochopitelně obávají jeho dalšího omezení. Vypadá to téměř tak, jakoby v česku, kde jsou veřejnoprávní instituce kritizovány za kde co, měly najednou větší důvěru, než ty americké v USA.

9 SPOLUPRÁCE BEZPEČNOSTNÍCH SLOŽEK

9.1 Orgány činné v trestním řízení

Pro potřeby pochopení součinnosti orgánů kybernetické bezpečnosti s orgány činnými v trestním řízení je třeba charakterizovat vztah pojmů kybernetická bezpečnost a kybernetická kriminalita. Kybernetická kriminalita a kybernetická bezpečnost jsou oblasti, které jsou jen těžko oddělitelné v propojeném prostředí kyberprostoru. Tento fakt je mimo jiné reflektován i v Rezoluci Valného shromáždění OSN ke kybernetické bezpečnosti z roku 2010[255], ve kterém se o kybernetické kriminalitě hovoří jako o jedné z hlavních výzev kybernetické bezpečnosti. Boj proti kybernetické kriminalitě je rovněž integrální součástí strategie národní kybernetické bezpečnosti a ochrany kritických infrastruktur[256]. Konkrétně předpokládá především přijetí vhodné legislativy směřující proti škodlivému zneužívání informačních a komunikačních technologií k páchání trestných činů, vytvoření vhodných personálních a technických prostředků na úrovni orgánů činných v trestním řízení, zajištění potřebných organizačních změn, vybudování mechanismů spolupráce se zainteresovanými subjekty a rovněž prostředků pro efektivní mezinárodní spolupráci.

V českém prostředí ke krokům směřujícím k zajištění těchto požadavků již delší dobu dochází. Již v roce 2005 došlo ze strany ČR k podpisu Úmluvy o kyberkriminalitě[257], která signatářské státy zavazuje k přijetí legislativních změn umožňujících stíhání kybernetických trestných činů. Přestože k ratifikaci úmluvy Českou republikou došlo až v roce 2013, většina ustanovení hmotného i procesního páva trestního byla zahrnuta do české trestněprávní úpravy již dříve. Specifickou úpravu obsahuje především trestní zákoník, který umožňuje stíhat například trestné činy neoprávněného přístupu k počítačovému systému či nosiči informací, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, či poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

255 Rezoluce Valného shormáždění OSN ze dne 17. března 2010 (64/211) „Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures".

256 Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, dostupné online zde: https://www.govcert.cz/download/gov-cert/container-node-id-998/nskb-150216-final.pdf.

257 Úmluva o počítačové kriminalitě ze dne 23. 11. 2001 (ETS No. 185).

Poněkud problematičtější je situace v případě procesních ustanovení. Ačkoliv předkládací zpráva k ratifikaci úmluvy konstatuje soulad české právní úpravy s jejími požadavky[258], nelze s jejími závěry tak docela souhlasit. Úmluva totiž požaduje, aby signatářské státy zavedly procesní nástroje umožňující orgánům činným v trestním řízení přikázat správcům uchování dat, vyžadovat vydání dat, vydat příkaz k vyhledání a zajištění dat a k odposlechu a sběru provozních dat. Aby však mohly české orgány činné v trestním řízení tyto v úmluvě poměrně detailně popsané procesní úkony realizovat jsou v současné situaci nuceny v podstatě „ohýbat" aktuální instituty trestního práva procesního. Například zajištění dat uchovávaných u ISP se na úrovni jednotlivých policejních obvodů realizuje prostřednictvím různých procesních nástrojů, ke sjednocení realizace zajištění emailových dat muselo být vypracováno stanovisko Nejvyššího státního zastupitelství[259] a v neposlední řadě nástroj, kterým by mohly orgány činné v trestním řízení přikázat ISP uchování uživatelských dat prakticky neexistuje. Česká republika si je však do určité míry těchto nedostatků vědoma a proto v současné době odborná pracovní skupina organizovaná pod Ministerstvem spravedlnosti pracuje na aktualizaci úpravy trestního řádu, která by měl alespoň některé z nich legislativně řešit.

Z organizačního hlediska k vývoji rovněž dochází. Klíčové postavení v rámci Policie ČR má v současnosti Národní centrála proti organizovanému zločinu, která vznikla v roce 2016 sloučením Útvaru pro odhalování organizovaného zločinu (ÚOOZ) a Útvaru odhalování korupce a finanční kriminality (ÚOKFK). Ta se jako ústřední orgán specializuje mimo jiné i na boj s počítačovou kriminalitou a plní i koordinační roli. Významnou roli hraje rovněž Útvar zvláštních činností, který provádí odposlech a záznam telekomunikačního provozu, sledování osob a věcí a další specializované úkony směřující k zajišťování elektronických důkazů. Na lokální úrovni rovněž vznikají, nebo jsou posilovány Odbory informační kriminality na krajských ředitelstvích kriminální policie. Na úrovni státního zastupitelství a soudů začala Justiční akademie realizovat specializovaná školení a na Nejvyšším státním zastupitelství vznikla neformální odborná skupina zaměřené na počítačovou kriminalitu.

Aby však mohly orgány činné v trestním řízení efektivně plnit svoji nezastupitelnou roli v zajišťování kybernetické bezpečnosti musí mít kromě technického a personálního vybavení a kvalitního legislativního zázemí rovněž dostatek informací o jednáních, která mohou mít povahu trestného činu v příslušných infrastrukturách. Proto je klíčové sdílení informací s orgány a subjekty kybernetické bezpečnosti. Problematika spolupráce dohledových pracovišť kybernetické bezpečnosti s orgány činnými v trestním řízení je intenzivně řešena nejen

258 Viz online zde: http://www.senat.cz/xqw/webdav/pssenat/original/66810/56264.
259 Stanovisko NSZ č. 1/2015.

v České republice, ale i na mezinárodní úrovni. Europol ve spolupráci s agenturou ENISA pořádá pravidelná setkáni, na kterých se projednávají především mechanismy pro předávání relevantních informací o kybernetických útocích[260].

V ČR je tato problematika řešena od počátku účinnosti ZoKB zejména z hlediska toho, co by měl NBÚ respektive národní CERT reportovat policii a současně k jakým datům z evidence kybernetických bezpečnostních incidentů by měla mít policie přístup.

První otázka je značně problematická díky veřejnoprávní povaze NBÚ. Ust. § 8 odst. 1 totiž ukládá státním orgánům povinnost neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin. Vzhledem k tomu, že množství nahlášených kybernetických bezpečnostních incidentů může být velmi velké a vzhledem k tomu, že vysoké procento jich může nasvědčovat spáchání trestného činu, mohlo by se velmi snadno stát, že bude policie povinně realizovanými oznámeními neúměrně zahlcována, neboť každé oznámení představuje poměrně intenzivní administrativní zátěž. Mnohé incidenty totiž, ač mohou indikovat trestný čin, nemá smysl vůbec hlásit, ať již proto, že pravděpodobnost dopadení pachatele je prakticky nulová, nebo proto že pravděpodobnost úspěšné kvalifikace daného incidentu podle trestního zákoníku je nízká. Hledají se proto mechanismy, jak standardizovat postupy a hodnotit jednotlivé incidenty z pohledu trestního práva. Jedním z podpůrných prostředků, který je v současné době silně podporován ze strany Europolu, je vytvoření taxonomie kybernetických bezpečnostních incidentů s navázáním na úpravu trestního práva. V České republice byl návrh takové taxonomie vytvořen Českým centrem excelence pro kybernetickou kriminalitu[261], ta klasifikuje nejen kybernetické bezpečnostní incidenty ve smyslu ZoKB, ale zohledňuje i jiné škodlivé aktivity, které mohou dohledová centra kybernetické bezpečnosti detekovat. Jednotlivé typy aktivit pak definuje a spojuje s příslušnou právní úpravu ZoKB a trestního zákoníku a doporučeními z hlediska vhodného postupu bezpečnostního týmu jak s ohledem na zachování existence důkazního materiálu tak s ohledem na ochranu infrastruktury. Klasifikace jednotlivých aktivit dle trestního práva je pak rovněž doplněna o specifikaci znaků příslušných skutkových podstat, aby mohl bezpečnostní tým vyhodnotit, zda taková aktivita může či nemůže být trestným činem. Aktuální návrh předmětné taxonomie kybernetických útoků je přílohou této publikace.

260 Za tímto účelem má dokonce Europol a ENISA sjednánu dohodu o strategické spolupráci. Dostupné online zde: https://www.europol.europa.eu/newsroom/news/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol.

261 Jde o výzkumné centrum Ústavu výpočetní techniky Masarykovy univerzity. Více viz http://www.c4e.cz.

Skupina	Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení
Sběr informací	Scanning	Aktivní nebo pasivní shromažďování informací o informačních systémech a počítačových sítích, prostřednictvím kterého lze získat informace o zranitelnostech předmětných systémů	✓	✓		
	Sniffing	Odposlouchávání všech protokolů, které počítač přijímá / odesílá pomocí počítačového programu, nebo hardwarového zařízení, takzvaného snifferu (používá se např. pro odposlouchávání přístupových jmen a hesel, čísel kreditních karet).	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je-li to prakticky možné, neznemožňovat okamžitě zařízení realizaci sniffingu - může být za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.
	Phishing	Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat.	✓	✓	Jde o typ ostatní kybernetického bezpečnostního incidentu způsobeného kybernetickým útokem. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.	Je vhodné zajistit obsah podvodných zpráv a služeb zajistit pokud možno včetně zdrojových kódů. Před znemožněním jejich provozu je vhodné kontaktovat PČR, která může zajistit vysledování přenosu zneužitých údajů a případně tak identifikovat pachatele.

Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li scanning prováděn za účelem získání informací sloužících k sestavení postupu využitého následně k provedení neoprávněného přístupu k počítačovému systému či nosiči informací (§ 230), nebo k odposlechu datové komunikace (§ 182)
Pasivní analýza sniffovacího zařízení - zde v podstatě žádné riziko nehrozí. Představuje-li však sniffovací zařízení počítačový systém, který je opatřen bezpečnostním opatřením zamezujícím přístupu, mohla by analýza dat, ke kterým je získán přístup překonáním takového opatření, vést k naplnění znaků skutkové podstaty trestného činu dle § 230 TZ - Neoprávněný přístup k počítačovému systému a nosiči informací. Aktivní protiopatření s trasováním útočníka - běžné trasování a blokování komunikace by němělo být problematické. Bude však postup vyžadovat přístup do šifrované komunikace, či bude-li přistupováno do počítačového systému útočníka po překonání bezpečnostního opatření nebo za účelem získání dat, opět hrozní naplnění skutkových podstat trestných činů porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu do počítačového systému.	§ 182 - Porušení tajemství dopravovaných zpráv	Je-li odchytávána datová zpráva přenášená elektronickou sítí konkrétnímu uživateli, nebo jde-li o odchytávání datového přenosu do, z, nebo uvnitř počítačového systému
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Výroba, držení, nebo distribuce nástroje ke sniffingu v úmyslu spáchat TČ porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu k systému. Může jít také opatření hesla prostřednictvím sniffingu v úmyslu spáchat TČ neoprávněného přístupu k systému.
	§ 234 - Neoprávněné opatření, padělání a pozměnění platebního prostředku	Je-li prostřednictvím siffingu získán platební prostředek (platební karta, elektronické peníze apod.) bez souhlasu oprávněného držitele. Trestná je i příprava tohoto TČ.
Bude-li prováděna aktivní analýza s přístupem k útočníkovu systému, nebo systému hostujícímu podvodnou stránku, může dojít k naplnění znaků skutkové podstaty TČ dle § 230 TZ. Zajištění komunikace podvodné stránky, nebo poškozeného s útočníkem, může být rovněž vyhodnoceno jako zásah do telekomunikačního tajemství a jako TČ dle § 182 TZ.	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Jsou-li prostřednictvím phishingu získávány přístupové údaje k přístupu do počítačového systému, nebo k nosiči informací za účelem spáchání trestných činů podle § 230 nebo § 182.
	§ 209 - Podvod	Je-li poškozený uveden útočníkem v omyl, na základě kterého mu vznikne škoda - například bude útočník v rámci phishingu vyžadovat zaslání finanční hotovosti.
	§ 234 - Neoprávněné opatření, padělání a pozměnění platebního prostředku	Jsou-li prostřednictvím phishingu získávány údaje o platebních kartách, nebo přístupové údaje do internetového bankovnictví

Skupina	Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení
Škodlivý kód	Virus, Trojan, Spyware	Virus = typ malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací. Trojský kůň = Program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje. Spyware = program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval.	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je vhodné zajistit kopii škodlivého software, která může sloužit k další analýze jako zdroj důkazního materiálu a k identifikaci pachatele. Je-li to prakticky možné, nelikvidovat okamžitě malware z napadeného systému - může být za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.
	Distribuce	Distribuce škodlivého software prostřednictvím sítí, nebo datových nosičů, s cílem infikovat škodlivým kódem hostitelský systém.	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je vhodné zajistit kopii škodlivého software, která může sloužit k další analýze jako zdroj důkazního materiálu a k identifikaci pachatele. Je-li to prakticky možné, nelikvidovat okamžitě malware z napadeného systému - může být za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.
	C&C	Command and control je informační systém, ze kterého je řízeno fungování sítě zařízení infikovaných škodlivým software.	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je vhodné informovat policii ještě před zneškodněním command and control centra. Je-li například hostováno na spravovaném zařízení nebo ve spravované síti, může jeho monitoring významně přispět ke zjištění pachatele, nebo k lokalizaci poškozených systémů.

Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty
Anaýza malware - neměla by být problematická, pokud v rámci ní není malware šířen, nebo nezpůsobí škodu. Aktivní protiopatření s trasováním útočníka - běžné trasování a blokování útočníka by nemělo být problematické. Bude-li však postup vyžadovat přístup do šifrované komunikace, či bude-li přistupováno do počítačového systému útočníka, nebo jiného napadeného, po překonání bezpečnostního opatření, nebo za účelem získání dat, opět hrozí naplnění skutkových podstat trestných činů porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu do počítačového systému.	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Dochází-li prostřednictvím škodlivého software k neoprávněnému přístupu k systému po překonání bezpečnostního opatření, nebo je-li přístupem neoprávněně nakládáno s daty v napadeném systému.
	§ 209 - Podvod	Některé typy škodlivého software vyžadují zaslání finanční částky od uživatele například za účelem získání přístupu k jeho datům nebo jako pokutu za neoprávněné užívání software - jde o takzvaný ransomware. Zpravidla lze tyto aktivity kvalifikovat jako podvod.
	§ 182 - Porušení tajemství dopravovaných zpráv	Některé typy malware mohou sloužit také k odposlechu komunikace napadeného systému, v takovém případě lze kvalifikovat dle § 182 TZ.
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li škodlivý software vyráběn, distribuován, nebo držen s úmyslem páchat jeho prostřednictvím TČ neoprávněného přístupu k počítačovému systému a nosiči informací.
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li škodlivý software vyráběn, distribuován, nebo držen s úmyslem páchat jeho prostřednictvím TČ neoprávněného přístupu k počítačovému systému a nosiči informací.
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Při distribuce malware dochází k neoprávněnému v kládání dat do počítačových systémů, lze tedy kvalifikovat jako TČ dle § 230 odst. 2 TZ
Snaha o nabourání do systému, který funguje jako command and control systém škodlivého botnetu, i za účelem zajištění bezpečnosti a dostupnosti spravovaných aktiv může být kvalifikována jako TČ dle § 230 TZ.		

Skupina	Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení
Dostupnost	DoS, DDoS	Technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.	✓		Jde o typ ostatní kybernetického bezpečnostního incidentu způsobeného kybernetickým útokem. Jde o kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv.	Platí stejná doporučení jako u CandC
	Sabotáž	Plánovaný útok cílený na poškození systému, přerušení procesu, nebo změnu či smazání informací.			Může jít o kybernetický bezpečnostní incident způsobený porušením organizačních opatření, nebo spojený s projevem trvale působících hrozeb. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti, dostupnosti či integrity aktiv.	
Pokus o průnik	Využívání zranitelností	Pokus o průnik do systému nebo sítě zneužitím zranitelností systému, jeho komponent, nebo sítí. K těmto pokusů může docházet pomocí exploitů, SQL injection, XSS, file inclusion apod.	✓	✓	Je-li průnik neúspěšný, jde toliko o kybernetickou bezpečnostní událost. Úspěšný průnik znamená kybernetický bezpečnostní incident způsobený překonáním bezpečnostního opatření, který způsobuje narušení důvěrnosti aktiv.	
	Pokus o přihlášení	Pokus o přihlášení do služby nebo získání přístupu k systému nebo síti. K těmto pokusům může docházet například při využití techniky brute force, slovníkového útoku, nebo odhadování hesla.	✓	✓	Pokud jde o neúspěšné přihlášení, jde toliko o kybernetickou bezpečnostní událost. Úspěšné přihlášení znamená kybernetický bezpečnostní incident způsobený překonáním bezpečnostního opatření, který způsobuje narušení důvěrnosti aktiv.	
Průnik	Využívání zranitelností	Průnik do systému nebo sítě realizovaný za zneužití zranitelností systému, jeho komponent, nebo sítě. K těmto útokům může docházet pomocí exploitů, SQL injection, XSS, file inclusion apod.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.	
	Zneužití účtu	Průnik do systému nebo sítě prostřednictvím zneužití uživatelského nebo administrátorského účtu.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti či integrity aktiv.	

Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty
Distribuovanému útoku DoS jde zabránit efektivně v podstatě jedině zneškodněním CandC centra ovládaného útočníkem, jeho zpětné trasování a samotné zneškodnění předpokládá přístup obránce do počítačových systémů třetích stran, nebo útočníka, což lze kvalifikovat jako TČ dle § 230 TZ.	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	K útoku DoS může docházet při využití explitu za účelem vyčerpání zdrojů napadeného systému, pak lze kvalifikovat dle § 230 odst. 1 písm. a), nebo pomocí zahlcení napadeného systému požadavky ze externích zařízení (například při využití botnetu), pak lze kvalifikovat dle § 230 odst. 1 písm. b)
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Ať již jde o útok zvenčí nebo zevnitř organizace a nezávisle na tom, zda jde o vandalismus, nebo cílenou snahu poškodit systémy nebo datový přenost, lze vždy kvalifikovat některou ze skutkových podstat § 230 TZ.
	§ 232 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	Je-li například za výskyt incidentu odpovědný správce který zanedbal svoje povinnosti a v té souvislosti umožnil vznik incidentu.
	Shodně jako Průnik - ve stádiu pokusu	
	Shodně jako Průnik - ve stádiu pokusu	
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Všechny techniky takto mohou být kvalifikovány, buď při neoprávněném přístupu dochází k obcházení zabezpečení, nebo dochází k modifikaci nebo nakládání s daty systému.
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	I když je přístup neúspěšný, samotné využívání nástrojů při pokusu je dokonaný TČ dle § 231 TZ.
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Podaří-li se do systému vstoupit, nebo přidat, upravit, nebo smazat data.
	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Podaří-li se získat přihlašovací údaje k systému za účelem páchání další trestné činnosti.

Skupina	Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení
Informační bezpečnost	Neautorizovaný přístup	Neoprávněný přístup k určité sadě informací.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.	
	Neautorizovaná modifikace/smazání	Neautorizovaná změna nebo likvidace určité sady informací.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti, dostupnosti a integrity aktiv.	
Podvod	Zneužití nebo neautorizované využití zdrojů			✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu může jít o kybernetický bezpečnostní incident způsobující narušení dostupnosti a integrity aktiv.	
	Neoprávněné využití jména třetí strany				Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.	
Škodlivý obsah	Spam	Hromadné rozesílání nevyžádaných zpráv elektronickými prostředky – nejčastěji elektronickou poštou.			Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.	
	Duševní vlastnictví	Protiprávní užívání duševního vlastnictví - především šíření rozmnoženin autorských děl (audiovizuálních, software apod.), či jejich zpřístupňování.		✓	Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.	
	Dětská pornografie, rasismus, schvalování násilí	Šíření závadného obsahu různého druhu, především zakázané pornografie, xenofobní a rasistické zprávy, podněcování k násilí apod.		✓	Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.	
Jiné	Jiné					

Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Je-li překonáno bezpečnostní opatření.
	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Vždy § 230 odst. 2 TZ.
	§ 268 Porušení práv k ochranné známce a jiným označením	
	Šíření spamu jako takové není trestným činem. Jeho obsah však může některé skutkové podstaty naplňovat, například v případech phishingu.	
	§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi	
	Hlava III. a hlava XIII.	Různé trestné činy - například šíření pornografie, výroba a jiné nakládání s dětskou pornografií, projev sympatií k hnutí směřujícímu k potlačení lidských práv apod.

Druhá problematická oblast, tedy přístup orgánů činných v trestním řízení do evidence kybernetických bezpečnostních incidentů vedené NBÚ souvisí především s výkladem ust. § 9 odst. 3 ZoKB, který ukládá NBÚ, aby poskytoval údaje z evidence incidentů orgánům veřejné moci pro výkon jejich působnosti. Problematický je totiž mechanismus a rozsah přístupu k těmto údajům. Orgány činné v trestním řízení by pochopitelně ocenily neomezený přístup ke všem údajům v neomezeném rozsahu, NBÚ se však poměrně oprávněné může obávat, že by ztratila při takto širokém zpřístupnění velmi důležitou důvěru na straně povinných osob. Proto se hledá mechanismus zpřístupnění takových dat a vhodný model spolupráce. I v tomto případě jde o problém, který se netýká pouze ČR a i v tomto případě je řešen na úrovni Europolu a agentury ENISA přičemž jako vhodný nástroj se z jejich pohledu jeví automatizovaný elektronických nástroj k důvěrnému sdílení dat. Jeho specifika jsou však v současné době předmětem debat a lze jen těžko odhadovat jaký bude jejich výsledek.

9.2 Zpravodajské služby

V České republice působí celkem tři státní zpravodajské služby – Bezpečnostní informační služba, která vykonává funkci civilní kontrarozvědky, Úřad pro zahraniční styky a informace vykonávající funkci civilní rozvědky a Vojenské zpravodajství, kterému se věnuje následující podkapitola. Jejich postavení, působnost a fungování upravuje obecně zákon č. 153/1994 Sb., o zpravodajských službách České republiky.[262]

Bezpečnostní informační služba (BIS) je zpravodajská instituce České republiky, která působí uvnitř jejího území. Službu řídí a kontroluje vláda ČR a její fungování upravuj zákon č. 154/1994 Sb., o Bezpečnostní informační službě. BIS podle § 5 odst. 1 písm. d) zákona č. 153/1994 Sb., o zpravodajských službách ČR mimo jiné zabezpečuje informace o činnostech, jejichž důsledky mohou ohrozit bezpečnost nebo významné ekonomické zájmy České republiky. BIS se na základě tohoto mandátu zabývá např. šetřením nejrůznějších druhů elektronických útoků s dopadem na chráněné zájmy ČR, shromažďováním a analýzou informací o reálných či potenciálních hrozbách a rizicích souvisejících s provozováním strategických informačních a komunikačních systémů, jejichž zničení či narušení by mohlo mít

262 Podrobněji ke struktuře a fungování zpravodajských služeb viz POKORNÝ, L. Zpravodajské služby, Praha: Auditorium, 2012.

vážný dopad na bezpečnost či ekonomické zájmy ČR. Především se pak zaměřuje na systémy úřadů a institucí veřejné správy či dalších právnických osob, včetně soukromoprávní sféry, u kterých se předpokládá zvýšená ochrana v souvislosti s jejich významem či ve vazbě na jejich potenciální zařazení mezi subjekty kritické infrastruktury ČR.

Úřad pro zahraniční styky a informace (ÚZSI) je zpravodajskou službou České republiky, jejímž prvořadým cílem je zabezpečovat pro ústavní činitele a orgány státní správy České republiky včasné, objektivní a kvalitní zpravodajské informace, které mají původ v zahraničí a jsou důležité pro bezpečnost a ochranu zahraničně politických a ekonomických zájmů České republiky. Pro fungování ÚZSI neexistuje specifický předpis, a tak je jeho působnost upravena zákonem č. 153/1994 Sb., o zpravodajských službách České republiky. Sám Úřad svoji působnost v rámci kybernetické bezpečnosti nedeklaruje, nicméně se účastní budování systému kybernetické bezpečnosti v ČR ve spolupráci s ostatními zpravodajskými službami a NBÚ.

Podobně jako je tomu v případě orgánů činných v trestním řízení je hlavním problematickým bodem v rámci spolupráce NBÚ se zpravodajskými službami otázka sdílení informací. Zpravodajské služby z podstaty své činnosti mají tendenci veškeré informace utajovat respektive pro adresáty „předzpracovat", současně však vyžadují přístup k co nejširší paletě zdrojů. Nejinak tomu je v oblasti kybernetické bezpečnosti. A i v tomto případě je hlavní otázkou sdílení informaci z evidence kybernetických bezpečnostních incidentů. Jak již bylo řečeno ZoKB ukládá NBÚ tyto informace sdílet s orgány veřejné moci, které je potřebují pro výkon svých povinností, ale neupravuje postupy jak by mělo ke sdílení docházet. Primárním problémem tu však je především otázka dostatečného utajení aktivit zpravodajských služeb. Zatímco orgány činné v trestním řízení zpravidla nemají problém požadované informace dostatečně identifikovat, u zpravodajských služeb je tomu jinak. I samotná informace o tom, na jaké infrastruktury se zaměřují či jaká data vyžadují by mohla znemožnit realizaci rozvědných činností, proto mají tyto služby snahu získat k evidenci přístup neomezený a nesledovatelný. Avšak i tady naráží na snahu NBÚ udržet v rámci povinných osob a bezpečnostní komunity dostatečnou vzájemnou důvěru, neboť si uvědomuje, že kdyby o ni přišla, bude spolupráce, která nyní probíhá i na neformální úrovni výrazně problematičtější.

9.3 Kybernetická obrana

Vedle kybernetické bezpečnosti je na národní i mezinárodní úrovni silně diskutovaným tématem kybernetická obrana. Vztah těchto dvou pojmů není jednoznačný, dají se ale obecně rozlišit tak, že kybernetickou obranou se rozumí využívání technických a netechnických nástrojů obrany státních zájmů v kybernetickém prostoru za účelem ochrany systémů které jsou pro jeho fungování kritické[263]. Zpravidla se o kybernetické obraně hovoří v souvislosti s aktivitami vojska. Ačkoliv je kybernetická obrana zmíněna v českém Akčním plánu k národní strategii kybernetické bezpečnosti, definice tohoto pojmu se nedočkáme. Aktuální právní úprava pojem kybernetické obrany rovněž neobsahuje a absentuje i jakákoliv regulace. V rámci Akčního plánu byla však gesce nad kybernetickou obranou přiznána Vojenskému zpravodajství, které je jednou ze tří zpravodajských služeb České republiky. Bylo zřízeno zákonem č. 289/2005 Sb., o Vojenském zpravodajství (dále též „ZoVZ"), a je jednotnou ozbrojenou zpravodajskou službou České republiky integrující rozvědnou i kontrarozvědnou činnost. Součástí Vojenského zpravodajství má být podle Akčního plánu nově zřízené Národní centrum kybernetických sil, které má zajišťovat po technické stránce aktivity směřující k vybudování prostředků kybernetické obrany. Aby však mohlo toto centrum fungovat, předpokládá i Akční plán přijetí příslušné právní úpravy, která by Vojenské zpravodajství vybavila mandátem a procesními nástroji.

V současné době je tato právní úprava již v počátcích legislativního procesu v podobě návrhu novely ZoVZ. Tento návrh jde cestou definování pojmu kybernetické obrany, svěření jejího zajišťování Vojenskému zpravodajství jako součásti Ministerstva obrany a úpravy prostředků, které budou sloužit k zajišťování kybernetické obrany.

Podle tohoto návrhu má být pojem kybernetické obrany definován v zákoně č. 222/1999 Sb., o zajišťování obrany České republiky jako „souhrn činností a opatření směřujících k vytvoření účinného systému obrany v kybernetickém prostoru a příprava a použití sil a technických prostředků kybernetické obrany podle zákona o Vojenském zpravodajství". Má ji zajišťovat Vojenské zpravodajství a to pomocí technických prostředků kybernetické obrany.

263 Viz např. definice v Národní strategii Francie pro obranu informační infrastruktury.

Těmi pak mají být věcné technické prostředky vedoucí k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany České republiky. Aby mohly být takové prostředky efektivně využívány zahrnuje navrhovaná právní úprava i povinnost ISP podnikajících podle ZEK zřízení a zabezpečení rozhraní pro připojení technických prostředků kybernetické obrany, kteří budou mít nárok na účelně vynaložené náklady. To však výlučně na základě schválení vládou, která rovněž schválí podmínky jejich používání k zajištění kybernetické obrany.

Pokud bude hrozit, že by využití těchto prostředků mohlo narušit důvěrnost zpráv podle zákona o elektronických komunikacích a s nimi spojených provozních a lokalizačních údajů konkrétní osoby, bude je moci využívat Vojenské zpravodajství na území České republiky jen výlučně za podmínek stanovených pro použití zpravodajské techniky, tedy až po svolení předsedy senátu Vrchního soudu v Praze.

Tato podoba návrhu novely je výsledkem připomínkového řízení, které bylo poměrně bouřlivé. Poměrně nepřekvapivě se k návrhu kriticky vyjadřovalo především Ministerstvo spravedlnosti, Český telekomunikační úřad, či Bezpečnostní informační služba[264]. Ač jde v této podobě o určitý kompromis, který by schválen legislativní radou vlády[265], nedá se považovat za zcela bezproblémový. Největší obavy z jeho podoby mají pochopitelně ISP, kteří se obávají, že bude aktivitami Vojenského zpravodajství zasahováno do důvěrnosti elektronických komunikací[266]. Mimo jiné rovněž argumentují, že nelze zajistit, že monitoring datového provozu prostřednictvím vágně definovaných technických prostředků bude skutečně neadresný a nebude umožňovat identifikaci konkrétních uživatelů. Navíc návrh nikterak neupravuje na jakou dobu, nebo v jakém rozsahu by mohl být neadresný monitoring bez souhlasu soudu provozován, respektive jak by se rozlišovala data adresná a neadresná.

264 Viz připomínky zveřejněné v aplikaci o/dok dostupné online zde: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl & p_p_lifecycle=0 & p_p_state=-normal & p_p_mode=view & p_p_col_id=column-1 & p_p_col_count=3 & _material_WAR_odokkpl_pid=ALBSA9LJNBUU & tab=remarks.

265 Viz stanovisko předsedy legislativní rady vlády ze dne 30. září 2016.

266 Viz například připomínky ICT Unie dostupné online zde: http://www.ictu.cz/fileadmin/user_upload/documents/Stanoviska___Komentare/2016/2016-05-23-HK-102_16-pripominky_ICTU.pdf.

10 VYMEZENÍ ZÁJMU STÁTU V KYBERPROSTORU

V následujících kapitolách bude pozornost věnována otázce realizace zájmů České republiky v kyberprostoru, zejména s přihlédnutím k mezinárodnímu právu veřejnému a k jeho případné aplikaci na kybernetické operace. Otázku, zda se mezinárodní právo na tyto operace aplikuje, lze mít za vyřešenou, jak bude uvedeno dále. Nicméně nevyřešené zůstávají některé otázky směřující ke způsobu a rozsahu aplikace. Nejednoznačný zůstává také postoj České republiky k této problematice.

Následující text je koncipován ve třech tematických celcích. Prvním z nich (kap. 10) je suverenita a způsob, jakým si Česká republika svoji suverenitu v kyberprostoru naformulovala, tedy skrze hodnotové nastavení kybernetické bezpečnosti jako nástroje k ochraně informačního sebeurčení. Druhým z nich (kap. 11) je otázka aplikovatelnosti *ius ad bellum* na kybernetické operace, kde se zabýváme zejména termínem kybernetické války a aplikovatelností právního rámce zapovídajícího využití síly. Termín kybernetické války je z pohledu práva nerelevantní, spíše potenciálně nebezpečný – má v sobě určitý senzační a mobilizační nádech, který zveličuje hrozby a je schopen potlačit racionální diskuzi o aplikovatelnosti existujících pravidel. Ta je přitom potřeba, protože dosavadní pravidla jsou zaměřena na kinetické násilí, zatímco kybernetické operace budou ve většině případů nekinetické. Ve třetím celku (kap. 12) se pak věnujeme hodnotovému pozadí *ius in bello*, které spatřujeme ve využívání tzv. Martensovy klauzule. Pozornost je také věnována aplikaci konkrétních pravidel, zejména těch směřujících k oddělení vojenských cílů od civilních objektů a civilní populace, což je vzhledem k často opakované potenciálně nediskriminační povaze kybernetických operací důležité téma pro nastolení právního rámce, ve kterém se budoucí operace musí odehrávat.

10.1 Kybernetická a informační suverenita

Suverén představuje na určitém teritoriu nejvyšší autoritu. Tato definice jako taková představuje to, co Philpott označuje jako „moderní notaci politické

autority".[267] Veškerá činnost, jejíž projevy pozorujeme jako praktický chod institucí nebo jako politické myšlení, směřují k tomu, co chápeme jako vytvoření a udržení suverenity nad daným teritoriem. Tři prvky vyskytující se v definici pak představují tři atributy, které směřují k ustavení skutečné suverenity.

Prvním atributem je bezesporu autorita jako právo rozkazovat a k němu korespondující (a, zejména, vynutitelné) právo být poslechnut. Druhým atributem je míra této autority – má (a musí být) nejvyšší. Ten, komu svědčí suverenita, je nejvyšší z autorit. Philpott upozorňuje, že toto vnímání autority je vlastní moderně. Ta byla schopna oprostit se od mnohosti autorit založených feudálně, kanonicky či jinak – žádná z nich tak vlastně nebyla v žádný okamžik *nejvyšší* v moderním státovědném pojetí.[268] Třetím atributem suverenity je pak vázanost autority ke konkrétnímu území, tedy ke konkrétní fyzické lokalitě. Suverén pak představuje nejvyšší autoritu pouze v rámci vymezeného území a ten, kdo aspiruje na pozici suveréna, musí všechny tyto atributy naplňovat.

Ve vztahu ke shora uvedeným atributům je nutné poznamenat, že jakkoli je vnímáme jako pevné a neměnné, podléhají ve zcela zásadní míře dynamice. Již Oppenheim připustil, že stát může přestat být státem ve chvíli, kdy z něj emigruje veškeré obyvatelstvo.[269] Tím by se vytratil i suverén, protože nelze ovládat či vládnout neadresně. V dnešní době reálně čelíme hrozbě zaplavení nízko položených ostrovů v důsledku globálních klimatických změn, což s sebou ponese ztrátu území a tím i ztrátu suverenity v jejím běžném chápání.[270] Také můžeme sledovat situace, kdy suverén představuje nejvyšší autoritu nad územím, které ale není vymezeno zcela bez diskuzí – je vymezeno pouze přibližně, bez přesně zaměřených hranic, které mohou být předmětem sporů se sousedy. Jestli je teritorium větší či menší nemá na moc suveréna nad daným územím žádný vliv. Stejně tak jsme měli možnost

267 PHILPOTT, Daniel. Sovereignty. *Stanford Encyclopedia of Philosophy*, publikováno 2003, upraveno 2016. Dostupné z: http://plato.stanford.edu/entries/sovereignty/

268 Tamtéž.

269 OPPENHEIM, Adolf Leo. *International Law: A Treatise*. New York and Bombay: Longmans, Green, and Co., 1905. S. 117 (marg. č. 79). Dostupné z: https://archive.org/details/internationallaw12oppe.

270 WONG, Derek. Sovereignty Sunk? The Position of 'Sinking States' at International Law. *Melbourne Journal of International Law*, 2013, roč. 14, č. 2, s. 346-391.

diskutovat, jaký vliv na suverenitu má fakt, že celní a poštovní služby vykonává pro suveréna někdo jiný. Se vznikem EU jsme se ve vztahu k členským státům staly svědky diskuze o určité omezené, neabsolutní, suverenitě.

Tato suverenita představuje nejvyšší moc nad daným územím, ale nikoli ve všech aspektech. Tato omezenost – jakási neabsolutní forma suverenity – je významným posunem od Bodina či Hobbse, kteří právě suverénovi ukládali nejvyšší moc nad všemi oblastmi. K tomuto posunu ve vnímání suverenity se vyjádřil MacCormick[271] tak, že ve vzdání se části suverenity není možné bez dalšího spatřovat problém. Naopak – je nutné ji vnímat jako jediné rozumné východisko pro budoucnost. Takováto omezené míra suverenity se často stává apelem národoveckých uskupení – vměšování do vnitřních záležitostí nemůže přece žádný stát strpět, tvrdí. Jakýkoli stát je suverénní ve chvíli, kdy ho žádná vně stojící moc nemůže omezit ve výkonu moci vnitřní,[272] kdy je od vnějších vlivů de facto osvobozen.[273] Tuto tradicionalistickou pozici dnes nelze vnímat zcela bez kontroverze.

Počátkem shora uvedené teze o oddělení vnitřní moci, jejímž je suverén zdrojem, od vnější moci, již se musí podřídit, je v hrubých (až mytických[274]) rysech Vestfálský mír. Právě po roce 1648 se totiž inference do záležitostí jiného státu stala nelegitimním nástrojem. Dnes je suverenita normativně zakotvena v Chartě OSN, zejména ve čl. 2 odst. 4, který zapovídá státům útoky na politickou nezávislost a teritoriální integritu – čl. 2 odst. 7 pak zakazuje intervence. MacCormick v rámci výše uvedené přednášky vlastně kritizoval tezi státu jako absolutního a ničím neomezeného suveréna, kterému se přisuzuje absolutní politická i normativní moc. Tento stav dle MacCormicka marginalizuje vliv mezinárodního práva, primitivního práva, kanonického práva, ale také existenci faktických pravidel nebo existenci

271 MACCORMICK, Neil. Beyond the Sovereign State. *Modern Law Review*, 1993, roč. 56, č. 1, s. 1-18.

272 Tamtéž, s. 14.

273 Jako ústavní nezávislost konstituuje vnější suverenitu James v JAMES, Alan. The Practice of Sovereign Statehood in Contemporary International Society. *Political* Studies, 1999, roč. 47, č. 3, s. 460-462.

274 Tento výraz je zde na místě – Vestfálský mír je v jeho interpretaci jako zásadního momentu pro vliv moderního chápání suverenity spíše mytický. Srov. DE CARVALHO, Benjamin, HALVARD, Leira a John M. HOBSON. The Big Bangs of IR: The Myths That Your Teachers Still Tell You about 1648 and 1919. *Millenium*, 2011, roč. 39, č. 3, s. 735-758.

sociálních institucí.[275] Potřeba přesné identifikace počátku všeho ve smyslu zdroje moci, vede ke ztotožnění veškerého práva se státem. Také vede k intuitivní potřebě z vnějšku neomezeného suveréna – co je naše, nám, chtělo by se říci. Proto je apel na udržení suverenity ve své podstatě primitivní a proto je určitá míra omezení suverenity cestou, která umožňuje vývoj. Na druhé straně je nutné přiznat, že z hlediska mezinárodního práva můžeme v tomto pojetí pozorovat jistou nestabilitu – permanentní bitvu politických mocí. Intervence do záležitostí jiného státu totiž mohou být vedené jak altruismem, snahou zabránit genocidě či chránit lidská práva, tak politickým realismem nebo individuálními ambicemi.

Jak jsem již naznačil, EU, které se tak obsáhle věnoval MacCormick, není prvním ani jediným projevem omezení moci suveréna. Do určité míry je možné postupné omezování moci chápat jako trend, který je spojený s vývojem po roce 1945, kdy dochází k přenášení části suverenity států na mezinárodní organizace.[276] A to i v intencích přístupu na vlastní území – státy musí strpět přístup na území kvůli kontrole vývoje zbraní hromadného ničení apod. Hobbsův Leviathan, tento smrtelný bůh, se tak stává minulostí. MacCormick vidí stín Leviathana za hrozivými zkušenostmi obou světových válek.[277] Tato zkušenost nás tak, alespoň ideově, vzdaluje od glorifikace politického realismu a tím i od absolutní moci suveréna. MacCormick uvedl, že se nacházíme v čase překonání suverénního státu[278]– dostali jsme se za zrcadlo a musíme hledat cestu vpřed. Tato cesta nás vede pryč od mýtu, který má jediný reálný význam při vznášení nároků státu na konkrétní území, jak cynicky poznamenal Lauterpacht.[279]

Tuto erozi Leviathana pozorujeme s nárůstem vojenských operací, které zasahují do svrchovanosti států za účelem nápravy – za všechny jmenujme operace v bývalé Jugoslávii, Libyi nebo v Iráku. Praktika intervence

275 MacCormick 1993 op. cit., s. 14.
276 Viz FINNEMORE, Martha a Kathryn SIKKINK. International Norm Dynamics and Political Change. *International Organization*, 1998, roč. 52, č. 4, s. 887-917. Také LAUTERPACHT, Eli. Sovereignty-Myth or Reality. *International Affairs*, 1997, roč. 73, č. 1, s. 141.
277 MacCormick 1993 op. cit., s. 17.
278 Tamtéž, s. 18.
279 Leuterpacht 1998 op. cit., s. 149.

z pohnutek stojících mimo „hmatatelné“[280] zájmy suveréna se stává poměrně častou a projevuje se v ní moralismus – snad posun k suverénovi, který není Leviathanem, ale instrumentáriem pro realizaci cílů vlastních obyvatel.[281] Je samozřejmě možné, že tento moralismus je pouze maskou, za kterou se skrývá kalkul. Obecně je ale možné říci, že demokratické státy společně sdílí ideu, že čím méně anarchie je pozorováno v mezinárodních vztazích, tím více jsou chráněny jejich vlastní zájmy. Čím méně pistolníků dělá z mezinárodního kolbiště Divoký západ, tím více je přítomno racionálních hráčů a tím jednodušší je vyjednávání. Moralismem motivované intervence tak samozřejmě mohou být projevem politického realismu – nepřiznaného či dokonce nevědomého.

Vývoj směřující k „očesávání“ suverenity, tomuto svlékání a porcování Leviathana, nás vede ke konstrukci křehkého mezinárodního společenství, ve kterém jsou jednotliví suveréni omezování. Nikoli snad proto, aby se z nich staly dobré a demokratické státy (tato moralistická pozice je samozřejmě možná, ale velice nepravděpodobná), ale proto, abychom se vyvarovali excesů, ve kterých divocí pistolníci práskají dveřmi od saloonu a vypouští rakety do moře poblíž Japonska. K tomuto ostatně dospěl v minulosti již Hugo Grotius, když připustil potrestání krutého prince princi vládnoucími v okolí.[282] Možná ale Leviathana není nutné přímo porcovat – Jouvenel, stojící proti Hobbsově ideálu, nenavrhoval odvržení suverenity jako takové. Spíše směřoval k její redefinici tak, aby bylo zajištěno, že suverén nebude chtít nic jiného, než to, co je legitimní a dobré.[283] Přirozenoprávní suverén přijímá přirozenou validitu morálky – nemusí ji validovat sám. Odvržení části suverenity ve prospěch mezinárodních organizací je tak do jisté míry možné chápat jako cestu tímto směrem. Odstranění části moci suveréna, spoutání Leviathana řetězem, který způsobí úbytek pistolníků, ani by přímo musel

280 Srov. šest principů politického realismu – MORGENTHAU, Hans Joachim. *Politics among nations: the struggle for power and peace*. Boston: McGraw-Hill, 1993.

281 Stát slouží občanům a nikoli obráceně – Viz ANNAN, Kofi. Two Concepts of Sovereignty. *The* Economics, 1999, 16th September. Dostupné z: http://www.economist.com/node/324795

282 Philpott 2016 op. cit.

283 Viz DE JOUVENEL, Bertrand. *Sovereignty: An Inquiry Into the Political Good*. Chicago: University of Chicago Press, 1957. S. 201 (citováno dle Philpott 2016 op. cit.).

existovat šerif – MacCormick roztomile uvádí, že suverenita je v tomto případě jako panenství, protože fakt, že o ni někdo přišel, neznamená, že ji někdo získal.[284]

Do tohoto trendu v současné době přichází kybernetická bezpečnost a informační kontrola. Ne snad proto, že by kontrola informací byla novinkou, ale proto, že nikdy nebylo jednodušší informace šířit, ať už k dobrému nebo zlému (oba tyto hodnotové soudy budou mít samozřejmě diametrálně odlišné významy při pohledu zástupců různých supervelmocí). Informační suverenitu chápeme jako extenzi suverenity ve vztahu k informacím – tedy ke vstupům rozhodovacích procesů na různých mocenských úrovních. Gong formuloval tezi, že informační suverenita by měla být nejvyšší informační mocí v informační politice ve státě a zároveň nejvyšší autoritou pro udržení informačního pořádku ve státě.[285] Jak je uvedeno výše, informační suverenita není novou ideou – již vypuštění Sputniku přineslo uvědomění si možnosti satelitů pro mezinárodní komunikaci, ale i pro politickou rovnováhu. Objevily se hlasy konstatující ohrožení národní suverenity s proliferací západních technologií – tyto technologie s sebou totiž pochopitelně nesly příslušné kulturní produkty. Zde není nutné hledat úmysl v podobě státem řízené propagandy, ale spíše fakt, že kulturní tvorba pocházející z určité země, přesněji řečeno kulturní oblasti, s sebou nutně musí nést jisté artefakty, které tuto kulturu vystihují. I toto pak může být chápáno jako ohrožení informační suverenity.[286]

Současný tlak na liberalizaci internetu a striktní síťovou neutralitu tak mohou některé státy vnímat, zejména pokud jsou ve vztahu k informační infrastruktuře státy rozvojovými, jako útok na svá práva a na svoji bezpečnost.[287] Kontrola nad přeshraničním tokem informací, kterou Gong označuje

284 MacCormick 1993 op. cit., s. 16

285 GONG, Wenxiang. Information Sovereignty Reviewed. *Intercultural Communication Studies*, 2005, roč. 14, č. 1, s. 119-135. S. 120.

286 Srov. UNESCO Declaration of Guiding Principles on the Use of satelite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange z roku 1972, dostupné z http://unesdoc.unesco.org/images/0000/000021/002136eb.pdf. Nejzajímavější jsou konkrétně čl. 2 a čl. 6. Zajímavá je pak i volba o tomto dokumentu – 55 hlasujících bylo pro, 7 proti, 22 se zdrželo. USA bylo v minoritě, zatímco SSSR se hlasování zdržel.

287 Gong 2005 op. cit., s. 126.

za měkkou informační suverenitu,[288] představuje kontrolu nad politickými, kulturními či sociálními informacemi. Realizují se v ní kulturní tradice, ideologie či politický systém[289] – jako taková je tato měkká informační suverenita méně způsobilá k nalézání konsenzu a ke spolupráci.[290] Rozsáhlou informatizací byla tato sféra informační suverenity do jisté míry „zestátněna" v tom duchu, že se stala státním zájmem a stala se tak předmětem politických, ekonomických, kulturních či vojenských úvah.

Tofflerův poměrně senzační závěr o tom, že právě rozdíly v názorech vedou ke konfliktům a mohou vést k nejhorším krveprolitím následujících let,[291] do jisté míry reflektuje ideu Leviathana. Hobbsův Leviathan jako jediný nastoluje řád v pustině, ve které je člověk člověku vlkem. Bodinův suverén pak jako jediný přichází s odpověďmi na základní otázku života, vesmíru a vůbec.[292] V tomto směru je zajímavým závěr estonského prezidenta Toomase Hendrika Ilvese, který pronesl v odpovědi na dotaz na konferenci CyCon v Tallinnu v roce 2016. Dle něj je v Kantovském světě plném ideálů při hledání viníka důležitá kauzalita – na straně druhé je v „*Hobbesovské pustině bez práva*" důležitá korelace.[293] Informační a kybernetická suverenita nás tak, minimálně dle uvedených slov, částečně vrátila v čase. Hobbes je zde vnímán jako politický realista – stát státu vlkem v mezinárodních vztazích. Kant zde pak vystupuje jako univerzalista, který neakcentuje konfliktní povahu mezinárodního práva, ale vnímá ho jako zájem všech lidských bytostí. Tato idea je do značné míry vtisknuta ve Všeobecné deklaraci lidských práv jako globálním poutům Leviathana. Přitom existuje i třetí přístup – mezi Hobbsem a Kantem stojí Grotius, jehož internacionalismus neakcentuje konflikt ani společné zájmy, ale přirovnává stav ke hře. Ta je částečně distributivní

288 Tamtéž, s. 127.
289 Tamtéž.
290 Tamtéž.
291 TOFFLER, Alvin a Heidi TOFFLER. *War and antiwar.* New York: Warner Books, 1993. S. 27.
292 Srov. MacCormick 1993 op. cit., s. 15.
293 Viz práci Geerse a kol., kteří pozorovali korelaci mezi prohlubováním politické krize na Ukrajině a počtem tzv. callbacků od infikovaných počítačů v rámci botnetů využívaných pro DDoS útoky – GEERS, Kenneth, THOMPSON, Kevin a Abhishek PIDWA. *Leviathan? Command and Control Communications on Planer Earth.* Black Hat Las Vegas, 2014. Dostupné z: https://www.blackhat.com/docs/us-14/materials/us-14-Geers-Leviathan-Command-And-Control-Communications-On-Planet-Earth-WP.pdf.

a částečně produktivní. Gong uvádí na příkladu Číny, že nutný je relativní a nikoli absolutní koncept informační suverenity.[294] Ta má být pragmatická[295] a v Grotiově duchu umožnit užší spolupráci. Stát, který se vzdává absolutní kontroly ve sféře, kterou mu nezapovídají univerzalistické nástroje, získává zpět něco na oplátku.[296]

V právu tyto úvahy materializují výrazně pomaleji a vývoj v oblasti kybernetické bezpečnosti stále výrazně ovlivňuje právní nejistota. Za výchozí bod, jakýsi *de lege lata* standard, je možné přijmout pravidlo č. 1 v Tallinnském manuálu, které uvádí, že stát může vykonávat kontrolu nad informační a komunikační infrastrukturou a nad aktivitami v ní v rámci vlastního suverénního území.[297] Tato definice přímo vychází z klasického rozhodnutí *Island of Palmas* z roku 1928, kde bylo uvedeno, že suverenita značí nezávislost – ta se pak váže k teritoriu a značí, že stát je oprávněn vykonávat tam nerušeně funkce státu.[298]

Tallinnský manuál tak v rámci *de lege lata* analýzy uvádí, že kyberprostor je neoddělitelně závislý na „železe", na konkrétním hardwarovém vybavení, které vždy má geografickou polohu. Nelze nevzpomenout na anekdotu, kterou dává napříč svými přednáškami a kurzy k dobru Michael Schmitt, editor Tallinnském manuálu – dle jeho vlastních slov byla jeho počáteční právě s termínem *cloud computingu* poměrně rozpačitá. Netušil totiž, že *cloud computing* znamená, že data jsou na nějakém konkrétním území, jen je problematické v daném okamžiku zjistit, kde přesně se nacházejí. Ve chvíli, kdy se dozvěděl technologické implikace termínu, nad kterým právě bádal, hodil celou svoji dosavadní práci do koše a začal znovu.

Tallinnský manuál spojuje informační a kybernetickou suverenitu s tradiční suverenitou vztaženou k určitému území. Podrobuje danou infrastrukturu

294 Gong 2005 op. cit., s. 133.
295 Tamtéž.
296 Tamtéž. Shodně Lauterpacht 1997 op. cit., s. 141 – tyto výhody mohou být někdy i nehmotné v tom smyslu, že benefity plynoucí z lidskoprávních závazků jsou politicky skutečné a významné, ale nejsou změřitelné v ekonomickém slova smyslu.
297 SCHMITT, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. S. 15 (pravidlo 1).
298 Viz Islands of Palmas case (Netherlands, USA). *Reports of International Arbitral Awards Vol. II pp. 829-871*. United Nations: 1928 (2006). Dostupné z: http://legal.un.org/riaa/cases/vol_II/829-871.pdf. S. 838.

a veškeré informace, které se na ní nacházejí, právní i regulatorní kontrole daného suveréna. Touto logikou je státu dána možnost infrastrukturu a informace, které se na ní nacházejí, chránit, využívat nebo zneužívat.[299] Samotný fakt, že je komunikační infrastruktura provázána s globální komunikační sítí zde neznamená, že by se stát tímto vzdal svého suverénního postavení.[300] Pro výkon suverenity se uvažuje fyzická vrstva infrastruktury, tedy geografická lokalita „železa".[301] Manuál uzavírá, že operace vedená proti této infrastruktuře může narušovat suverenitu – tedy, že ji bude narušovat ve chvíli, kdy způsobí škodu.[302] Skupina expertů, která na Tallinnském manuálu pracovala, se však nedokázala shodnout, zda dojde k narušení suverenity i ve chvíli, kdy dojde např. k umístění kódu sledujícího provoz. Tento kód může sloužit k monitoringu aktivit v síti, ale nebude způsobovat přímou škodu (resp. škodu sekundárním kinetickým následkem[303]).

Zde opouštíme shodu a dostáváme se do vod spekulačních. Narušení suverenity totiž vnímáme právě přes její násilné dopady – očekáváme mrtvé, zraněné a zničenou infrastrukturu. Informační suverenita, nad jejímž vymezením se odborníci často nedokáží shodnout, ale nevyžaduje takto „tvrdý" zásah do suverenity státu. Moc můžeme jednoduše vnímat jako schopnost ovlivňovat chování jiných tak, abychom dosáhli kýženého efektu – v rámci takovéto definice ji nevnímáme v termínu mnohosti zdrojů moci, ale v jednotném termínu vlivu na chování.[304] Pro pochopení lze uvést příklad – pokud máme enormní množství zdrojů, ale chybí nám možnost, jak jich efektivně využít, nemáme moc ve vlivu na chování. Až efektivní alokace těchto zdrojů nám dává tento konkrétní druh moci. Snadná dostupnost komunikačních technologií snižuje náklady na dosažení moci v intencích vlivu na chování.

299 Tallinn Manual op. cit., s. 16 (pravidlo 1, odst. 5).

300 Tamtéž, s. 17 (pravidlo 1, odstavec 10).

301 Odvážnější úvahy, než se objevují v Tallinnském manuálu, můžeme pozorovat v práci ROWLAND, Jill, RICE, Mason a Sujeet SHENOI. Whither cyberpower? *International Journal of Critical Infrastructure Protection*, 2014, roč. 7, č. 2, s. 134-135. Autoři zde předkládají v zásadě dvě možnosti vývoje – (1) potvrzení primátu těla nad duchem (autoři nepoužívají toto označení) v podobě udržení teritoriality nebo (2) uvolnění tohoto prostoru státem a jeho zaplnění jinými (i nestátními aktéry). Ve druhé variantě by stát svoji suverenitu nad „železem" odmítnul a kyber-státem by se tak na jeho území mohl stát kdokoli.

302 Tallinn Manual op. cit., s. 16 (pravidlo 1, odst. 6).

303 O tom dále v textu.

304 NYE, Joseph. *The Future of Power*. New York: Public Affairs, 2011. S. 9-10.

Tento druh moci pak zasahuje do informační suverenity – omezuje schopnost suveréna být nejvyšší informační mocí v informační politice ve státě.[305] Dosažení informační suverenity umožňuje posílení či udržení moci, zatímco alternativní zdroje informací tuto moc, do značné míry, podrývají. Toto vše je řečeno bez ohledu na ideové pozadí – některé formy vlády tendují k informačnímu pluralismu, což nakonec ale stejně vychází z rozhodnutí suveréna nenárokovat si tuto formu suverenity pro sebe.

Z pozice mezinárodního práva (přesněji řečeno Charty OSN) se zdá, že nedestruktivní informační útoky nejsou problémem. Je totiž rozdíl mezi útokem a donucováním.[306] Zatímco útok s fyzickými následky (byť sekundárními, způsobenými manifestací škodlivého kódu) bude mezinárodně protiprávním chováním, donucení bez fyzického následku nikoli. Mezinárodní právo se tak možnosti rozšířeného narušení informační suverenity přizpůsobuje jen velmi obtížně.[307] Objevují se tak hlasy po významné redefinici normativního záběru zápovědi užití síly v mezinárodním právu tak, aby eventuálně mohlo pokrýt i narušení informační suverenity.[308]

Opačný názor prezentuje např. Buchan,[309] kdy nejdříve pesimisticky konstatuje, že k extenzivní reinterpretaci termínu *použití síly* nedojde,[310] ale vzápětí kontruje prohlášením, že i kybernetický útok bez fyzických následků (tedy i zásah do informační suverenity prostředky informačních a komunikačních technologií), může být za určitých okolností mezinárodně protiprávním činem[311] podle

305 Gong 2005 op. cit., s. 120.
Shodně BUCHAN, Russell. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict & Security Law, 2012, roč. 17, s. 223.

306 Viz BARKHAM, Jason. Information Warfare and International Law on the Use of Force. *New York University Journal of International Law & Politics*, 2001, roč. 34, č. 1, s. 84-85.

307 Tamtéž, s. 112.

308 Viz JOYNER, Christopher C. a Catherine LOTRIONTE. Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, 2001, roč. 12, č. 5, s. 825-865, zejména závěr na s. 864-865. Viz také HATHAWAY, Oona A., CROOTOF, Rebecca, LEVITZ, Philip a Haley NIX. Law of Cyber-Attack. C*aliforni*a Law Review*,* 2012, roč. 100, č. 4, s. 821.

309 Resp. nejenom on – Jensen např. prezentuje názor, že odlišný standard protože současné standardy jsou dostačující i ve vztahu k sekundárním následkům – JENSEN, Eric Talbot. Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? *American University International Law Review*, 2003, roč. 18, č. 5, s. 1145-1188.

310 Buchan 2012 op. cit., s. 214.

311 Tamtéž.

obyčejového zákazu intervence.[312] Buchan se v tomto odvolává na předchozí doktrinální práce[313] s tím, že ve chvíli, kdy je cílem operace vynutit si změnu v politice cíleného státu, může se jednat o dostatečnou míru zásahu, který může vést k závěru o mezinárodněprávní zápovědi takového jednání.[314] Buchan konstatuje, že příklad Estonska v roce 2007 mohl být za takovýto akt považován, přestože *stricto sensu* nezpůsobil škodu (tedy tu fyzickou[315]).[316] Útoky trvaly po dobu několika týdnů a Estonsko vzhledem k jejich paralyzujícímu efektu zvažovalo aktivaci článku 5 Smlouvy NATO – tyto akce pak měly konkrétní cíl, tedy dosáhnout změny rozhodnutí přesunout sochu bronzového vojáka na méně prominentní místo v rámci hlavního města Tallinnu.[317] Minimálně z pohledu Estonska se tak jednalo o vměšování do vnitřních záležitostí – bylo omezeno v možnosti rozhodnout se o umístění symbolu tím, že mu vnější moc za toto rozhodnutí znemožnila využívat preferovaného způsobu komunikace. Tím je, vzhledem k přezdívce E-stonsko pochopitelně, internet.

Sféra informační suverenity tedy zcela jistě existuje, byť jí zatím nebyla věnována taková pozornost – její narušení často neústí v mrtvé a zraněné nebo ve fyzické škody. Zároveň s tím si většina liberálních demokracií informační suverenitu neosobuje pro sebe. S rozvojem informační společnosti a se znovuoživením doktríny hybridní války[318] se situace nicméně mění a státy směřují k vymezení svých kybernetických a informačních zájmů.

10.2 Česká republika: hodnotové zakotvení

Vzhledem k obsahu předcházející části se domníváme, že konceptualizace informační či kybernetické suverenity je v současné době ještě před

312 Mezinárodní soudní dvůr. *Case Concerning Military and Paramilitary Activities in and against Nicaragua. Judgment of 27 June 1986*. Dostupné z: http://www.icj-cij.org/docket/files/70/6503.pdf. Odst. 202.

313 Zejména JAMNEJAD, Maziar a Michael WOOD. The Principle of Non-intervention. *Leiden Journal of International Law*, 2009, roč. 22, č. 2, s. 348.

314 Buchan 2012 op. cit., s. 224.

315 Srov. výklad v rámci Tallinn Manual op. cit., s. 46 (pravidlo 11, odst. 3).

316 Buchan 2012, op. cit., s. 226-227.

317 Jakkoli banálně to zní, bronzová socha měla zcela zásadní symbolickou hodnotu.

318 K termínu viz HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007. Dostupné z: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

námi. To ale žádným způsobem nebrání státům své zájmy v kyberprostoru deklarovat. Vzhledem k problematičnosti notace informační či kybernetické suverenity považujeme za nejjednodušší zkoumat, jakým způsobem se státy v kyberprostoru chovají a jakým způsobem vymezují své zájmy. Česká republika učinila zásadní krok ve vymezení svého suverénního zájmu o kyberprostor formulací národních bezpečnostních strategií, národních strategií kybernetické bezpečnost a také vytvořením právního rámce kybernetické bezpečnosti.[319] Z tohoto důvodu nepovažujeme za důležité ani tak přesné znění nakonec přijatého rámce, ale spíše úvahy, které vedly k jeho vytvoření právě v této podobě.

Úvahy o vytvoření právního rámce kybernetické bezpečnosti vycházely z přirozené tendence rozvoje společnosti k vyšší míře informovanosti. Tento trend, v jehož rámci pozorujeme rozvoj síťových modelů nahrazujících klasická hierarchická uspořádání,[320] výskyt a rozvoj participativních složek médií,[321] rozvoj nových forem vzdělávání či nové způsoby v produkci informačních statků,[322] je vyvoláván nejen rozvojem informačních a komunikačních technologií, ale zejména jejich dostupností. Změny, které máme možnost pozorovat, ovlivňují všechny sféry lidské činnosti a my tak můžeme mluvit o tzv. informační společnosti.[323]

Důležitým prvkem je jako součást hodnotového rámce v euroatlantickém prostoru svoboda jednotlivce. Informační společnost představuje společnost, která je bezprecedentním způsobem závislá na distribuci a zpracování informací. Závislost na informacích je tak klíčovým pojmovým znakem a z něj pak vyrůstají specifická práva, kterými se realizuje svoboda, a které formulují hodnotový rámec, který je vlastní informační společnosti. Tento hodnotový rámec se pak dá označit sběrným termínem informačního sebeurčení.

319 V podobě zákona č. 181/2014, o kybernetické bezpečnosti

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

321 MCLUHAN, Marshall. *Understanding media: the extensions of man*. Cambridge: MIT Press, 1995. S. 30 a násl.

322 BENKLER, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press, 2006.

323 Viz také BENIGER, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA, USA: Harvard University Press, 1986.

Pojem informačního sebeurčení se poprvé objevil v Německu v první polovině osmdesátých let. Spolkový ústavní soud vytvořením tohoto konceptu zohlednil obecný trend, kdy se zásahy do informační sféry[324] jednotlivců začaly objevovat nikoli ve formě individuálních excesů, ale jako systémový fenomén. Informační sebeurčení tak mělo začít fungovat jako katalog hodnot, který měl být protiváhou tohoto trendu. V rozhodnutí Spolkového ústavního soudu se mj. uvádí, že *„[o]chrana základních práv zahrnuje též způsobilost člověka určit v zásadě dostupnost a užití jeho/jejích osobních údajů.“*[325]

V současné době je pod rozsah tohoto termínu možné zahrnout nejen práva na ochranu vlastního soukromí a osobních údajů, ale i aktivní práva směřující ke zpracování údajů a získávání a vytváření informací. Jedná se ve své podstatě o pozitivně i negativně vymezenou možnost kontroly nad integritou vlastní informační sféry – zejména ve vztahu k rozsahu zásahů do ní. Pozitivně je vymezena garancí jednotlivých distributivních práv informační povahy a negativně je pak vymezena zákazem ostatních do této sféry zasahovat (což platí i pro stát).

Tento sběrný pojem není zcela neproblematický – jedním z negativních aspektů je jeho relativní neurčitost. Informační sebeurčení představuje stále se rozvíjející koncept informačních práv, jejichž konkrétní rozsah se mění v závislosti na používaných technologiích a na technologickém vývoji obecně. S rozvojem nových forem komunikace se rozvíjí i formy omezování informačních práv jednotlivce. Například dokud nebyl internet masově rozšířen, mělo jen omezený smysl uvažovat o přístupu k němu jako o integrální součásti informačního sebeurčení. Podobná je situace v případě biometrických údajů, kdy nebylo nutné řešit limity jejich použití, dokud se technologie na nich založené nestaly běžně dostupnými. V současné době není možné vyčerpávajícím způsobem popsat strukturální nebo pojmový rozsah informačního sebeurčení – pojetí informačního sebeurčení se může lišit v rámci jednotlivých právních tradic dle jejich vlastních převládajících tendencí.

324 K pojmu též KOOPS, Bert-Jaap, NEWELL, Bryce Clayton, TIMAN, Tjerk, ŠKORVÁNEK, Ivan, CHOKREVSKI, Tom a Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law* [přijato k publikaci]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043

325 Nález Spolkového ústavního soudu ze dne 15. 12. 1983, č. j. BverfGE 65, 1. Dostupné z: http://www.servat.unibe.ch/dfr/bv065001.html.
Překlad dle POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012. S. 325.

Euroatlantická orientace platného práva na člověka se projevuje i zde, kdy pod rozsah pojmu informačního sebeurčení neřadíme korporátní či státní informační práva. V současné době a v našem kulturním prostoru je možné za součást informačního sebeurčení označit následující distributivní práva primárně informační povahy:

- 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.[326]

Důležitost informačního sebeurčení jako katalogu distributivních práv tkví v komplexitě jeho pojetí. Právo na soukromí nebo právo na informace veřejného sektoru jsou samostatně stojící důležitá informační práva. Zdůrazněním jejich společné funkce a společného původu v rámci pojmu informačního sebeurčení je jim ale přiznáván společný původ a společný smysl a tím i společný význam. Komplexní efekt zde ústí ve vyšší intenzitu závažnosti informačního sebeurčení v porovnání se závažností a důležitostí jeho jednotlivých komponentů. Svoji roli zde hraje i fakt, že tato práva mají společný informační základ a tak se jediný faktický zásah může manifestovat jako zásah do vícero práv.

V České republice je rozvoj práva na informační sebeurčení (resp. konstatování jeho existence soudy) pomalejší, než v západních zemích. Koncept informačního sebeurčení v kontextu informačních a komunikačních technologií tak začíná přitahovat pozornost až v posledních několika letech. Získává na důležitosti v soudních rozhodnutích nejvyšších soudů i v akademické sféře. Rozhodovací praxe bohužel upřednostňuje jednu jeho složku, konkrétně ochranu soukromí. Tím se do určité míry degraduje komplexní povaha pojmu informačního sebeurčení, nicméně i výklad pojmu soukromí v poslední době získává na šíři, takže se postupem času může s informačním sebeurčením při některých extenzivních konceptualizacích plně překrýt.[327]

Za svého druhu revoluci se v České republice dal označit nález Ústavního soudu ve věci sp. zn. I. ÚS 22/10 ze dne 7. 4. 2010,[328] kdy soud přiznal

326 Polčák 2012 op. cit., s. 326-327.
327 Máme na mysli zejména typologii v Koops 2016 op. cit.
328 Nález Ústavního soudu ve věci sp. zn. I. ÚS 22/10 ze dne 7. 4. 2010 (N 77/57 SbNU 43).

ochranu individuální internetové konektivitě. Přístup k internetu zde Ústavní soud vyložil jako extenzi práva na vytváření a rozvíjení vztahů s dalšími jednotlivci, která je integrální součástí respektování soukromého života. Nález nebyl zcela bez opozice,[329] celkově však jeho logika reflektovala roli, kterou internetová konektivita hraje v soukromém životě jednotlivce i obecný přístup k rozvoji informační společnosti.[330]

Zmíněný nález nepředstavuje exces v rozhodovací praxi, ale je spíše vyústěním aktuálních trendů. Koncept informačního sebeurčení se v judikatuře Ústavního soudu objevuje i ve společensky a mediálně exponovaných záležitostech. Objevil se v nálezu Ústavního soudu ve věci sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2010.[331] 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., trestního řádu, v nálezu Ústavního soudu ve věci sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011.[332]

Informační sebeurčení jako katalog distributivních práv s převážně informační povahou představuje lidskoprávní koncept, který přímo vyrůstá z informační společnosti. Jednou ze základních materiálních funkcí státu je přitom zajišťování společenské reprodukce právě formou ochrany

329 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.
Viz Polčák 2012 op. cit., s. 326.

330 Za všechny příklady tendencí na poli individuálního připojení k internetu lze jmenovat zprávu o svobodě projevu 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. Viz LA RUE, Frank. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. UN General Assembly, 2011. Dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Tím narážel v době vzniku zprávy i na Francii, kde fungovala tzv. digitální gilotina. K tématu blíže HABER, Eldar. The French Revolution 2.0: Copyright and the Three Strikes Policy. *Harvard Journal of Sports and Entertainment Law*, 2011, roč. 2, č. 2, s. 298-339.

331 Nález Ústavního soudu ve věci sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011 (94/2011 Sb., N 52/60 SbNU 625).
Více viz MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů*. Brno: Masarykova univerzita, 2013.

332 Nález Ústavního soudu ve věci sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011 (43/2012 Sb., N 217/63 SbNU 483)

distributivních práv.[333] Jestliže je informační sebeurčení hodno o ochrany ze strany státu formou konstrukce nedistributivního práva,[334] tedy kybernetické bezpečnosti,[335] pak se také jedná o hodnotu, která bude narušována kybernetickými operacemi proti státu vedenými. Stejná infrastruktura, kterou se český stát zavázal chránit v rámci ochrany schopnosti plnit materiální funkce státu, bude logicky cílena kybernetickými operacemi.[336]

Informační sebeurčení jako hodnota mělo zásadní vliv na legislativní konstrukci kybernetické bezpečnosti. Důvodem byla snaha *a priori* posoudit proporcionalitu nezbytného zásahu do práv subjektů. Perfektní technokratická definice kybernetické bezpečnosti byla zformulována jako složená z prvků tzv. triády CIA[337] – tedy jako zajištění důvěrnosti (*confidentiality*), integrity a dostupnosti (*availability*).[338] Při snaze zajistit tyto hodnoty legislativně tak zákon nezbytně musel zasáhnout do některých práv,[339] což by při neexistenci širšího konsenzu nad mírou přípustnosti solidárního omezení svobod mohlo legislativní práce zhatit.

Důvěrnost, která se vyskytuje v rámci triády CIA, směřuje k ochraně uložených či přenášených dat před přístupem ze strany neautorizovaných osob.[340]

---

333 HOLLÄNDER, Pavel. *Základy všeobecné státovědy*. 3. vydání. Plzeň: Aleš Čeněk, 2012. S. 103-106.

334 Nález Ústavního soudu ve vci sp. zn. Pl. ÚS 32/95 ze dne 3. 4. 1996 (112/1996 Sb., N 26/5 SbNU 215).

335 Zákon č. 181/2014, o kybernetické bezpečnosti

336 V této logice je pak možné chápat i utajení přílohy, kterou se stanovují prvku kritické infrastruktury, protože jejich zveřejnění by mohlo vést k jejich sekuritizaci, což by z nich pak mohlo učinit cíle.

337 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. Viz BOSWORTH, Seymour; KABAY, M. E. (eds.). *Computer Security Handbook*. 4th Edition. Hoboken: John Wiley & Sons, 2002. S. 116-136.

338 Viz GRAHAM, James; HOWARD, Richard; OLSON, Ryan (eds.). *Cyber Security Essentials*. Boca Raton: CRC Press, 2011. S.1.

339 Viz např. GARTZKE, Erik. The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, 2013, roč. 38, č. 2, s. 41-73, kde na s. 50 autor uvádí: *„The United States and other nations have already begun expensive regormd to prepare for war over the internet, while some civil liberties have been curtailed on the ground that cyberwar may well constitute the next existential threat."*

340 Viz Graham 2011 op. cit., s. 4.

Pro zajištění důvěrnosti musí mít systém možnost ověřit totožnost uživatele, který žádá o přístup a také musí mít možnost vyhodnotit, zdali má uživatel dostatečně oprávnění k dané operaci. Těmto krokům se postupně říká autentizace a autorizace a představují inherentní součást důvěrnosti jakéhokoli systému. Součástí tohoto prvku tak může být plejáda opatření vedoucích k zajištění důvěrnosti, např. systém nakládání s hesly, nakládání se šifrovacími klíči, blokování USB portů pro zamezení připojení paměťového zařízení.

Druhou složkou triády je integrita, která představuje vlastnost systému, kdy je znemožněno pozorovaně měnit v něm uložená nebo jím přenášená data.[341] Úzce souvisí s již zmíněnou autorizací a autentizací, ale i s tzv. nepopiratelností.[342] Integrita systému je tak podstatná i pro právní jistotu jeho uživatelů. V rámci systému se zajištěnou integritou je možné identifikovat celý řetězec od původce zprávy, přes obsah zprávy až k identitě příjemce. Jen tak je možné zajistit kompletnost uložených a přenášených dat, resp. předejít jejich změně, ať už intencionální či nikoli. V případě, že skutečně ke změně dat dojde, v náležitě zajištěném systému bude tuto změnu možné zpozorovat.

Poslední složkou triády CIA je dostupnost. Je možné ji stručně shrnout jako požadavek, aby data v systému (nebo celý systém) byla dostupná ve chvíli, kdy je to potřebné ze strany oprávněného uživatele.[343] Je nutné zajistit spolehlivý přístup k datům a informačním službám nejen v kvantitativním měřítku. Důležité je i měřítko kvalitativní, kdy se zajišťuje existence adekvátní odezvy systému na požadavky oprávněných uživatelů.[344]

Zajištění důvěrnosti, integrity a dostupnosti určitých služeb je tedy cílem, ke kterému směřuje zákon o kybernetické bezpečnosti. Kompromitace důvěrnosti, integrity a dostupnosti zájmových služeb je pak naopak cílem kybernetických operací. Jak bylo výše zmíněno, představuje kybernetická

341 Viz tamtéž, s. 4-5.

342 Angl. Nonrepudiation. Jedná se o ověření úkonu, který byl proveden prostřednictvím informačních sítí. Zahrnuje potvrzení původce a zároveň i nezměněnost informací při přenosu. Je zajišťována především asymetrickým šifrováním (soukromý klíč k podpisu, veřejný klíč k ověření pravosti podpisu) či hashováním zprávy. Nástrojem pro zajištění je samozřejmě také elektronický podpis známý i v České republice. Viz tamtéž, s. 3.

343 Oprávněnost uživatele k přístupu je opět nutné ověřit za pomoci autentizace a autorizace.

344 Graham 2011 op. cit, s. 5-6.

bezpečnost nedistributivní informační právo.[345] Jako taková nemůže být legitimní, pokud není schopna ochraňovat a respektovat relevantní distributivní práva. Ryze instrumentální pojetí kybernetické bezpečnosti jako realizace státního zájmu v kyberprostoru může vést k nezohledňování práv občanů, např. formou excesivního sledování jejich činnosti nebo filtrování některého obsahu, nebo povinných subjektů, např. formou přikázání bezpečnostních opatření, která jsou ve zjevném nepoměru k rizikům.

Extenzivní a instrumentální nastavení kybernetické bezpečnosti by neobstálo v případném testu proporcionality, kterým by muselo v případě ústavního přezkumu projít. Legislativní úvahy směřující k vytvoření zákon o kybernetické bezpečnosti tak využíval v rámci dílčích kroků testu proporcionality – jeho jednotlivé složky zahrnují kritérium vhodnosti, potřebnosti a porovnání závažnosti obou v kolizi stojících práv.[346] V souvislosti s konstrukcí nedistributivního práva kybernetické bezpečnosti je možné také zmínit tzv. příkaz k optimalizaci[347] jako příkaz k využití všech možných prostředků za účelem minimalizace omezení jednoho práva v případě prioritizace jiného v rámci testu proporcionality. Zejména při rizicích plynoucích z některých specifických asymetrických konfliktů[348] se může příkaz k optimalizaci snadno změnit v test vyloučení extrémní disproporcionality. K tomu dochází v případě přezkumu legálně vytvořených tzv. šedých zón, jak je označuje Dyzenhaus.[349] V těchto situacích je formálně proporcionalitě, resp. možnostem legální ochrany učiněno zadost, ale systémově jsou kladené překážky, které znemožňují jejich efektivní využití. Česká republika však před tuto volbu tváří v tvář bezpečnostním hrozbám ještě nebyla postavena, a tak byl test proporcionality v nedeformované podobě integrální součástí tvorby zákona o kybernetické bezpečnosti. Stejně tak musí být test proporcionality integrální součástí jakýchkoli úvah na bezpečnostní témata, aby se zamezilo příliš širokému nastavení pravomocí, které bude nepropor-

345 Polčák mluví o „*nedistributivním právu s dominantně informačním charakterem*." Polčák 2012 op. cit., s. 343.

346 Nález Ústavního soudu ve věci sp. zn. Pl. ÚS 4/94 ze dne 12. 10. 1994 (214/1994 Sb., N 46/2 SbNU 57)

347 ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, 2011. S. 23.

348 Tedy nahrazení střetů stát vs. stát terorismem, kybernetickými útoky skupin různého charakteru, ale i zřejmého nepoměru ve zvolené taktice a strategii boje atd.

349 Srov. DYZENHAUS, David. *Legality in a Time of Emergency*. Cambridge: Cambdridge University Press, 2006. S. 17-60.

cionálně omezovat v opozici stojící distributivní práva (svobodu pohybu, projevu, soukromí apod.). Z toho důvodu také spadají pod rozsah zákona o kybernetické bezpečnosti jen určité poměrně úzce vymezené subjekty, které jsou navíc systematicky odstupňovány podle důležitosti, která je jim v rámci zajištění kybernetické bezpečnosti přisuzována.[350]

Povinné subjekty podle zákona o kybernetické bezpečnosti tak v současné době zahrnují:

- poskytovatele služeb elektronických komunikací ve smyslu zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů,[351]
- orgány nebo osoby zajišťující významnou síť,[352]
- správce informačního systému kritické infrastruktury,[353]
- správce komunikačního systému kritické infrastruktury[354]
- a správce významného systému informačního systému.[355]

Všem těmto druhově vymezeným subjektům navíc nebyly v zájmu proporcionálního šetření práv stanoveny povinnosti stejného rozsahu. Zákon o kybernetické bezpečnosti vymezuje subjekty pouze druhově a pro konkrétní vymezení povinných subjektů je nutné konzultovat jiné právní předpisy, popř. jiné dokumenty obecně. Seznam poskytovatelů služeb elektronických komunikací, kteří jsou, byť jen ve velmi omezené míře, povinnými subjekty, vede Český telekomunikační úřad. Tento seznam je veřejně dostupný.[356] Z hlediska informačních a komunikačních systémů, které jsou kritickými infrastrukturami, je řešení složitější, protože jejich konkrétní vymezení podléhá utajení, aby se zabránilo jejich sekuritizaci. Sekuritizace totiž, zjednodušeně řečeno, vede ke zvýšenému vnímání objektu jako cíle ve chvíli, kdy je označen za zájmový objekt z hlediska ochrany.[357]

350 Zjednodušeně řečeno, jinak vypadá test proporcionality pro subjekt povinný dle ust. § 3 písm. a) a jinak pro subjekt povinný dle ust. § 3 písm. c) zákona o kybernetické bezpečnosti.

351 Ust. § 3 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti

352 Ust. § 3 písm b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, významná síť je definována v ust. § 2 písm. g) téhož předpisu

353 Ust. § 3 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti

354 Ust. § 3 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti

355 Ust. § 3 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti

356 Evidence je dostupná na webových stránkách Českého telekomunikačního úřadu.

357 Viz HANSEN, Lene a Helen NISSENBAUM. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 2009, roč. 53, č. 4, s. 1155-1175.

Zákon o kybernetické bezpečnosti výrazně limituje technokratickou definici kybernetické bezpečnosti a zapracovává do její struktury relevantní hodnoty. Toto hodnotové pojetí kybernetické bezpečnosti směřuje nejen ke konstrukci kybernetické bezpečnosti v rámci informační společnosti a nikoli proti ní, ale také pomáhá definovat zájmy, které Česká republika považuje za důležité. Nikde tak nenajdeme poptávku po regulaci obsahu nebo dalších zásahů do informačního sebeurčení, které by byly s největší pravděpodobností v případě ústavního přezkumu považovány za neproporcionální stanovenému cíli, kterým je ochrana (kybernetické) bezpečnosti České republiky.

Absolutní pojetí suverenity státu, jehož mizení postupně pozorujeme, je rozvojem informační společnosti dále narušováno. Z konstatování, že informační sítě narušují státní hranice, se stává klišé využívané politiky, zpravodajskými službami, orgány činnými v trestním řízení a ostatně i občanskou společnosti. Konstatovat tak, kde přesně leží zájmy jednotlivých států v rámci kyberprostoru je kvůli konceptuální nevymezenosti pojmu informační suverenity netriviální úkol, který jde daleko za rámec tohoto textu. Na druhé straně je ale možné konstatovat, jakým způsobem k ustavení svých zájmů v kyberprostoru dospěla Česká republika. Právní rámec kybernetické bezpečnosti směřuje primárně na služby, které vnímáme jako důležité pro zajištění realizace hodnot informační společnosti. Stát nezasahuje na obsahovou úroveň a hlásí se k euroatlantické orientaci na lidská práva. Touto optikou je tak nutné realizaci informační suverenity České republiky i vnímat – jako ochranu práv obsažených v katalogu informačního sebeurčení. Na druhé straně je ale pravděpodobné, že toto vymezení zájmů České republiky z hlediska bezpečnosti povede k jejich sekuritizaci. Vymezený zájem se tak stane primárním cílem za situace, kdy někdo bude chtít využít kybernetických operací ke změně v politice země. Tomu je věnována další část textu.

11 KYBERNETICKÁ VÁLKA A POUŽITÍ SÍLY

11.1 Clausewitz a „kybernetická válka“

V rámci předchozí části jsme uvedli, že Česká republika se rozhodla realizovat svoji informační suverenitu hodnotovým vymezením kybernetické bezpečnosti. V rámci právního rámce, který byl produktem, definovala prvky, které považuje za důležité pro fungování státu a tím je vymezila jako objekty ochrany. Tím se ale informační suverenita nevyčerpává. Některé incidenty narušující důvěrnost, integritu a dostupnost služeb mohou dosahovat míry, která si vyžádá posouzení souladu operace s mezinárodním právem. Česká republika může být jejich cílem a v případě aktivní obrany teoreticky i původcem. Pokud je Česká republika na straně cíle, je právní posouzení důležité pro výběr adekvátní reakce. Pokud je Česká republika na straně původce, je právní posouzení důležité pro zabránění případné eskalaci mimo kyberprostor.

Pro klasifikaci kybernetických incidentů je možné použít různých kategorií, v jejichž rámci pak může vhodně zvolené spektrum přispět k jemnějšímu odlišení jednotlivých incidentů a tím i reaktivních či jiných opatření. Tikk navrhla kategorii rozdělující incidenty na porušení vnitřních předpisů, porušení právních povinností, kyberkriminalitu, kybernetický terorismus a kybernetickou válku.[358] Porušení vnitřních předpisů může v této kategorizaci představovat incident způsobený např. neopatrným nakládáním s hesly v rozporu s firemní bezpečnostní politikou či připojením neprověřeného nebo nezabezpečeného zařízení do interní sítě. Porušení právní povinnosti se může týkat např. nenahlášení kybernetického incidentu některým z povinných subjektů. Kybekriminalita pak bude, ze strany motivace původců, představovat incident vedoucí k osobnímu obohacení. Na normativní úrovni může spadat pod vymezení některé ze skutkových podstat trestního práva. Může se jednat o zvláštní skutkovou podstatu, např. neoprávněný přístup

358 TIKK, Eneken. *Comprehensive Legal Approach to Cyber Security*. Tallinn, 2011. Disertační práce, University of Tartu, Právnická fakulta. Dostupné z: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1. S. 69.

k počítačovému systému a nosiči informací, nebo o skutkovou podstatu, která může zahrnovat kriminální činnost za použití moderních technologií, např. poškozování cizí věci nebo podvod. S posledními dvěma kategoriemi pracuje Tikk tak, že kybernetický terorismus představuje ohrožení kybernetické bezpečnosti (zejména chodu kritických infrastruktur) vyvolané nestátními aktéry nezaměřenými na zisk a kybernetická válka pak představuje incidenty vyvolané státními aktéry. Zatímco první kategorie vyvolávají dojem triviálních přešlapů, rétorika posledních vyvolává dojem zásadních hrozeb pro chod státu. Právě v rámci poslední kategorie je možné představit si aplikaci mezinárodního práva. Následující text tak bude analyzovat pojem *kybernetické války* jako kategorie kybernetických incidentů. Další část pak bude analyzovat překryv tohoto pojmu s mezinárodněprávně relevantním pojmem *použití síly*.

Termín *kybernetická válka*, který se vyskytuje ve shora uvedené kategorizaci, se zdá být velmi populárním zejména v rovině propagace tématu kybernetické bezpečnosti státu. Narativ „kybernetického Pearl Harboru", který využil americký ministr obrany Leon Panetta v roce 2012, využívá popis možných tragických škod, které může na kritické infrastruktuře způsobit neočekávaný útok prostřednictvím kybernetických operací ze strany cizí mocnosti.[359] Jedná se přitom pouze o jeden z příkladů využití tohoto narativu, který je často motivovaný snahou svést se na vlně populárního tématu směrem k zajištění vyššího rozpočtu pro příslušnou organizaci.[360] Skepse k masivním škodám, které může kybernetická operace způsobit, vede i ke skepsi stranou samotného používání termínu kybernetické války.[361] Důvody ke skeptickému postoji se nicméně liší – jeden z názorů odmítající možnost rozpoutání kybernetické války je postaven na kritice příliš benevolentního používání pojmu válka, který ztratil na své konceptuální vyhraněnosti poskytnuté dílem Carla von Clausewitze.

359 *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City. October 11, 2012*. US Department of Defence. Dostupné z: http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

360 Srov. komentář LEE, Ronald M & Thomas RID. OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy. *The RUSI Journal*, 2014, roč. 159, č. 5, s. 4-12.

361 Srov. seznam kyberspektiků sestavený Johnem Muellerem a Benjaminem Friedmanem z CATO institutu na http://www.cato.org/research/cyberskeptics.

Varování před riziky plynoucími pro společnost z operací vedených proti rozvíjejícím se informačním a komunikačním systémům slýcháme nejméně od roku 1993. V roce 1996 si pak kybernetické hrozby vysloužily v USA pozornost, která vedla k ustavení zvláštní komise, která předložila svoji závěrečnou zprávu v říjnu 1997,[362] ve které byl konstatován nedostatek aktuální hrozby, ale tato nebyla do budoucna vyloučena. Postupně ale zájem o kybernetickou bezpečnost kritických infrastruktur rostl, stejně jako se vyvíjely i hrozby. V nedávné minulosti jsme se tak staly svědky operací, které manifestovaly do fyzického poškození provázaného vybavení.[363] Tyto možnosti, navíc představované jako zajištěné technickým a ekonomickým zázemí státního aktéra, manifestovaly do populárního termínu kybernetické války.

Rid je k používání tohoto slovního spojení velmi skeptický a při formulaci své pozice vychází právě z Clausewitzovy konceptualizace pojmu války.[364] Pravý a jediný smysl tohoto termínu totiž Rid spatřuje jako formulovaný dílem *Vom Kriege* tohoto pruského generála a skvělého stratéga. Tento příklon k minulosti v rámci snahy uchopit současné kybernetické hrozby přitom není zcela ojedinělý. Jakkoli jsou kybernetické operace projevem moderních technologií, někteří autoři při snaze popsat rizika z nich plynoucí a zformulovat operační a organizační protiopatření využívají *Umění války*.[365] Rid tedy extenzivně argumentuje Clausewitzem tak, že jakákoli akce, pokud míří k ustavení sebe sama jako aktu války, musí naplňovat tři základní kritéria.

Prvním z nich je násilný charakter takového aktu. *„Válka je aktem síly s cílem donutit protivníka, aby se podrobil naší vůli,"* stojí psáno na úvodní straně Clausewitzova životního díla. Násilí je tak základní ideou války a v tradičním chápání násilí znamená využití kinetických prostředků. Kybernetické operace, jak bylo v nedávné minulosti demonstrováno, mohou mít kinetické

362 President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* 1997. Dostupné z: https://www.fas.org/sgp/library/pccip.pdf.

363 Viz APPLEGATE, Scott. The Dawn of Kinetic Cyber. In: PODINS, Karlis; STINISSEN, Jan; MAYBAUM, Markus. *2013 5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2013. S. 165-167. Také PORSCHE, Isaac R. III, SOLLINGER, Jerry M., MCKAY, Shawn. *A Cyberworm that knows no Boundaries.* Santa Monica: RAND Corporation, 2011. Dostupné z: www.rand.org/pubs/occasional_papers/OP342.html

364 Viz Rid 2012 op. cit. s. 7.

365 Viz GEERS, Kenneth. *Strategic Cyber Security.* Tallinn: CCD COE Publications, 2011.

následky – to ve chvíli, kdy škodlivý kód manifestuje do fyzického poškození provázaného vybavení. Tyto případy jsou nicméně velmi vzácné a kód bude většinou využíván nekineticky. Může se jednat o sledování komunikace nebo dezinformaci podvržením dat. I z toho důvodu je v případě klasického chápání násilí odmítána možná násilná povaha kybernetických operací. Ve většině případů prostě kód nebude manifestovat na úrovni dostačující pro konstatování fyzického násilí. Proti této pozici se částečně vymezil Stone, který sice souhlasil, že pro válku je esenciální určitý vztah mezi silou, násilím a letalitou, zároveň ale uvedl, že válka zahrnuje i sílu, která nemusí představovat násilí – tedy alespoň ve smyslu, že by násilí mělo automaticky zahrnovat letalitu. Jedná se o tři odlišné koncepty a Stone tak kritizuje Rida za jejich nerozlišování.[366]

Rid v rámci tohoto prvního kritéria také připomíná Clasewitzovu premisu, že obě strany konfliktu se budou vždy pokoušet o eskalaci násilí do extrémů až do chvíle, kdy budou zastaveny politikou.[367] Eskalace kybernetických operací do kinetického (konvenčního) konfliktu je v dnešní době nežádoucí, nicméně některé státy již přímo možnost odpovědi konvenčními silami na kybernetické operace dosahující určité intenzity předpokládají.[368] Gartzke k možnosti eskalace nekonvenčních operací do konvenčního konfliktu dává zajímavý příklad. Dle něj je existence dostatečných konvenčních kapacit nástrojem pro odstrašení eskalace nekonvenčních (tedy i kybernetických) operací.[369] Schopnost potrestat cizí stát za narušení zájmů v určité doméně prostřednictvím

366 Viz STONE, John. Cyber War Will Take Place. *Journal of Strategic Studies*, 2013, roč. 36, č. 1, s. 101-108. S. 103-104. Dovozuje to ze zaměření Clausewitze na fyzickou sílu prostřednictvím častých analogií s fyzikálními silami.

367 Rid 2012 op. cit., s. 7.

368 Srov. *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. May 2011*. White House. Dostupné z: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. S. 14.
Na tuto strategii se odvolává také *The Department of Defence Cyber Strategy. April 2015*. Department of Defense. Dostupné z: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. S. 11
Srov. také *Wales Summit Declaration. September 2014*. NATO. Dostupné z: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.
Srov. také *Warsaw Summit Communiqué. July 2016*. NATO. Dostupné z: http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

369 Gartzke 2013 op. cit., s. 65

konvenčních sil tak částečně svědčí proti Ridově závěru o nemožnosti eskalovat konflikt. Je nicméně fakt, že tato eskalace je spíše v rovině spekulace; je politicky neprůchozí a i někteří odborníci před ní varují.[370]

Druhým kritériem je podle Clausewitze instrumentální charakter jednání, které má být vnímáno jako akt války. Fyzické násilí nebo hrozba fyzickým násilím zde představuje prostředek, zatímco účelem je akceptace vůle útočníka ze strany cíle aktu. Cíl aktu války musí být, jak uvádí Clausewitz, podrobení se politické vůli útočníka. V rámci kybernetických operací je v současné době možno způsobit minimálně částečnou neschopnost státu plnit svoje materiální funkce – značná část služeb, které moderní společnost vyžaduje, totiž potřebuje ke svému fungování nějakou formu informační nebo komunikační infrastruktury. Rid spatřuje zásadní limit při snaze splnit Clausewitzem definovanou instrumentalitu v chybějící schopnosti donutit oponenta ke změně politického kurzu. Ať už kybernetická operace vyvolává sekundární kinetický následek či nikoli, hrozba jejím provedením nebo její faktické provedení v případě kompetentního cíle efektivně znemožňuje její opakování. Škoda způsobená přes internet nebo podobné médium by měla politický význam a mohla by být vnímána jako akt války pouze ve chvíli, kdy by upravovala rovnováhu sil.[371] Nicméně ve chvíli, kdy je konkrétní kybernetická operace provedena a využívá určitých vlastností cíleného systému, schopný soupeř velmi rychle zavírá okno příležitosti a znemožňuje opětovné provedení operace.[372]

V rámci velice zjednodušeného pohledu je možné říci, že každá karta se dá hrát pouze jednou – Gartzke tuto situaci nazývá *use and lose* kapacitou.[373] Kybernetická operace se tak dá provést s cílem využít momentu překvapení, který pak může fungovat jako krátkodobá výhoda. Té je ale nutné okamžitě využít (např. nasazením konvenčních sil) nebo kompetentní protivník zavře okno příležitosti a daná operace se již nemůže opakovat.[374]

---

370 Waxman dokonce doporučuje rozpojení kybernetických operací s využitím konvenčních sil, aby k této eskalaci nemohlo dojít – viz WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law*, 2011, roč. 36, č. 2, s. 421-459. S. 453.

371 Gartzke 2013 op. cit., s. 57.

372 Tamtéž, s. 58.

373 Tamtéž, s. 60.

374 Došlo k odstranění zranitelností, vytvoření protiopatření apod. – Srov. tamtéž, s. 59.

Tím ztrácí svoji schopnost vyvolat změnu v rovnováze sil a tím pádem nemůžeme využít termínu *války*. Příkladem tohoto jednání jsou již shora zmíněné události z Tallinnu z roku 2007. Nepochybný moment překvapení nebyl dostatečně využit k vynucení útočníkovy vůle. Následný široký zájem o problematiku spojený s rozvojem kybernetických kapacit pak do značné míry znemožnil provedení podobné operace. Dá se říci, že největším rizikem pro vznik situace, kterou by bylo možné v Clausewitzových intencích označit za *kybernetickou válku*, je nezájem o problematiku. Pokud nedochází k rozvoji kybernetických kapacit, není cíl schopný zavírat okna příležitosti a útočník je schopen dosáhnout naplnění tohoto druhého kritéria.

Třetím kritériem je dle Clausewitze navazující politická povaha války. Účelem je vždy realizace politické vůle a každý válečný čin je tak nezbytně činem politickým. Clausewitzova nejcitovanější fráze, tedy že válka je pokračováním politiky jinými prostředky, nachází své uplatnění právě v tomto třetím kritériu. Zásadní otázkou pro schopnost manifestovat aktem politickou moc se zdá být schopnost přičitatelnosti aktu konkrétnímu státnímu aktérovi. Aby se totiž politická vůle za aktem stojící mohla manifestovat, akt musí být přičitatelný a jeho původce musí být komunikován.[375] Problém přičitatelnosti kybernetických operací je tak dvousečný – na jednu stranu do určité míry chrání původce před případnou odvetou, na druhé straně ale znemožňuje napadenému státu podvolit se útočníkovi, protože ten zůstává neznámý.[376]

V případě událostí v Estonsku v roce 2007 i v Gruzii v roce 2008 směřoval škodlivý provoz převážně z Ruska. Ze strany představitelů estonské vlády se ozývaly hlasy přirovnávající útoky k vojenskému zásahu, ale v tomto případě se jednalo vskutku spíše o vyjádření rétorického významu. Jedno z vyjádření nicméně Rid považuje za natolik důležité, že se vůči němu vymezil.[377] Rétorické cvičení jednoho z představitelů Estonska totiž zahrnovalo srovnání blokády přístavišť a námořních cest se zablokováním přístupu k informačním portálům.[378] Rid argumentuje, že na rozdíl od blokády přístavů není blokáda webů ani potenciálně násilná, s čímž nezbývá než souhlasit. Takovýto útok nemá ani sekundárně kinetické následky a provedené DDoS akce se nepodařilo provázat

375 Rid 2012 op. cit., s. 8.
376 Gartzke 2013 op. cit., s. 47.
377 Rid 2012 op. cit., s. 12-13.
378 Tamtéž, s. 13.

se žádným taktickým cílem. Rid zde zmiňuje, že ping zůstává anonymním.[379] V případě událostí v Gruzii Rid uzavírá, že efekty útoků byly malé, protože Gruzie nemá dostatečný přístup k internetové konektivitě ze strany obyvatelstva a celkově se v tomto duchu jedná o rozvojovou zemi.[380] Kybernetické operace byly doprovázeny konvenčními prostředky, které ale hrály v konfliktu rozhodující roli. Útoky tak, dle Ridova závěru, nebyly násilné ani instrumentálně vztažené k politické moci. Kybernetická válka zde tak představuje pojem spíše metaforický než deskriptivní.[381] Hlavní účel kybernetických operací vidí Rid v subverzi, špionáži nebo sabotáži a nikoli ve válce jako takové.[382] Ridova analýza tedy končí konstatováním, že existence kybernetické války není možná, protože kybernetické operace nejsou schopny kumulativně naplnit všechna tři kritéria formulovaná Clausewitzem. Ping zůstává anonymní a nemá politickou afiliaci. Na druhé straně, jak v Estonsku, tak v Gruzii korelovaly útoky s politickými cíli Ruské federace, jakkoli se v konkrétních případech nemuselo prokázat přímé spojení.

Jsme svědky trendu, který přesnou přičitatelnost útoku relativizuje a vyžaduje pouze korelaci s politickými cíli – zmínil to i Ilves ve výše uvedeném prohlášení. I v případě třetího kritéria tak může být jeho rozsah modifikován a za přičitatelnou (na politické úrovni ve vztahu k podrobení se moci) se začne považovat nikoli operace přímo spojená s jejím původcem, ale operace korelující s jeho deklarovanými zájmy. Tvrzení o nenaplnění Clausewitzova konceptu proto, že kybernetické operace dnes manifestují politickou vůli skrytě, máme za poměrně odvážné.

Clausewitzův koncept tak možná v dnešní době je stále ještě nepřekonaným, resp. představuje nejucelenější práci v oblasti filosofie války. Ale ve své čisté podobě, v jaké s ním pracuje Rid, se zřejmě nezachová. V závěru textu Rid označuje pojem kybernetické války za přísně metaforický bez deskriptivního přesahu – a toto tvrzení může být pravdivé. Nicméně není možné zcela vyloučit posun významu Clausewitze tak, aby odpovídal modernímu trendu kybernetických operací.

379 Tamtéž, s. 13.
380 Tamtéž, s. 14.
381 Tamtéž, s. 15.
382 Tamtéž. Srov. Stone 2013 op. cit., s. 105 – Stone zde naopak tvrdí, že sabotáž může být aktem války – u sabotáže cílíme na věci, nikoli na lidi, což je častým pojmovým znakem i v rámci kybernetických operací.

Co je ale nutné odmítnout je směšování teze o existenci kybernetické války s mezinárodněprávní povahou kybernetických operací. Clausewitz neztotožňoval svůj koncept s legalitou použitých prostředků, stejně tak legalitu nezohledňovali Rid ani Gartzke. V intencích naší současné zkušenosti je termín *válka* využíván pro zdůraznění mimořádného ohrožení – zařazení kybernetické války do klasifikace, kterou předložila Tikk, tak může směřovat k vymezení státního aktéra jako původce útoku, zároveň ale od takového jednání očekáváme určitou míru závažnosti. Označení s sebou obecně nese mnoho konotací, které sahají mimo normativní nebo deskriptivní význam pojmu, a mohou vést k vytvoření hysterického narativu – podobně jako ve shora uvedeném případu hrozby kybernetickým Pearl Harborem.

Některé kybernetické operace mohou být z pohledu mezinárodního práva veřejného legální, některé mohou být nelegální (o tom dále). Faktem je, že často korelují se zahraničně-politickými cíli konkrétních států, útočí na suverenitu a do značné míry realizují zahraniční a bezpečnostní politiku. Jestli tomuto druhu hrozeb budeme říkat *kybernetická válka* či nikoli není podstatné. Nevyužívání tohoto pojmu právě kvůli shora uvedeným konotacím zahrnujícím dojem maximálního nebezpečí pro výkon státní moci a zajištění funkcí státu se zdá být racionálním přístupem.. Povaha operací se využíváním přesnějšího termínu nezmění, stejně jako se nezmění jejich legalita. Kybernetické operace totiž už dnes mohou porušovat normy mezinárodního práva veřejného. Termín *kybernetické války* tak může plnit roli normativní, kterou ale dle Rida v současné době neplní. Může plnit roli agitační, za účelem získání dalších prostředků pro konkrétní organizace. Může plnit také roli deskriptivní - v tu chvíli ale může fungovat jako nežádoucí žurnalistická zkratka. Termín *kybernetická válka* v sobě zahrnuje dle Clausewitze jistou systematičnost – je pokračováním politiky jinými prostředky a má své cíle. I z toho důvodu je tento termín nepřesný a pro právní posouzení potenciálně nebezpečný. Aby byl totiž akt protiprávní, nemusí být *válkou*.

11.2 Kybernetická operace jako použití síly

Naplnění či nenaplnění Clausewitzových kritérií, jakkoli je zajímavou otázkou, nemá v podstatě žádný vliv na aplikovatelnost existující právní úpravy. Můžeme samozřejmě konstatovat, že jednání, které je absolutně nezpůsobilé

naplnit tento koncept, zřejmě nebude dostatečně závažné, aby na něj dopadalo mezinárodní právo veřejné. Nicméně se bude jednat spíše o korelaci, než o kauzalitu. Dle shora uvedeného navíc může být koncept naplněn, byť se jedná spíše o nepravděpodobné situace. S termínem kybernetické války tak je nutné zacházet velmi opatrně – nejenom vzhledem k jeho deskriptivní povaze pro právo, ale i vzhledem k negativním (až se chce říci senzacechtivým) konotacím. Otázka právní povahy kybernetických operací leží jinde, konkrétně ve výkladu pojmů použití síly (čl. 2 odst. 4 Charty OSN) a ozbrojeného útoku (čl. 51 Charty OSN). Tyto pojmy se totiž primárně vztahují k použití kinetických prostředků, byť přesah do prostředků nekinetických v podobě chemických či biologických zbraní registrujeme také.

Nekinetická povaha kybernetických operací je dovozována právě z jejich založení na počítačovém kódu, který je virtuální reprezentací konkrétních činností systému. Jak již bylo zmíněno výše, není možné konstatovat, že by ke kinetické realizaci kódu nemohlo docházet – kód může vyvolat činnosti, které budou mít kinetické následky. Primárním cílem takto motivovaných kybernetických operací tak budou CPS[383] systémy, které představují úzké propojení mezi počítačovým systémem a fyzickou infrastrukturou, např. v podobě SCADA[384] systémů řídících a monitorujících prvky kritické infrastruktury, ať už vodní, energetické či jiné. V minulosti byly některé z těchto možných způsobů útoku experimentálně ověřovány v řízeném prostředí[385] a byli jsme svědky i operačního nasazení podobných prostředků např. ve formě Stuxnetu.[386]

Pro potřeby mezinárodního práva je obecný zákaz hrozby nebo použití síly obsažen právě ve výše zmíněném čl. 2 odst. 4 Charty OSN. Tento zákaz je zde formulovaný jako pozitivní povinnost vyvarovat se v mezinárodním styku hrozby či použití síly jakýmkoli způsobem neslučitelným s cíli OSN. Zákaz hrozby nebo použití síly přitom není závazný pouze pro členské státy OSN, ale byl dovozen i jako mezinárodněprávní obyčej. Mezinárodní soudní dvůr zaujal stanovisko, že úprava obsažená v čl. 2 odst. 4 Charty

383 Angl., Cyber-physical systems.
384 Angl., Supervisory control and data acquisition.
385 Applegate 2013 op. cit., s. 165-170.
386 Tamtéž, s. 170-171. Pro analýzu Stuxnetu viz Porsche 2011 op. cit.

OSN v zásadě odpovídá zvykovému právu,[387] přičemž obecně je možné, aby smluvní a zvyková úprava existovala nezávisle na sobě. V otázce zákazu hrozby nebo použití síly se dle soudu obsah smluvního práva a zvykových norem liší, nicméně i při zcela stejném obsahu je možné aplikovat zvykové pravidlo separátně.[388]

Případnou pozitivní odpovědí na otázku aplikovatelnosti tohoto pravidla na kybernetické operace se problematika nevyčerpává. Jak poznamenal Koh, předmětem diskuze není ani tak, zda se mezinárodní právo na kybernetické operace aplikuje, ale jakým způsobem.[389] Charta OSN totiž byla sepsána v roce 1945, neobsahuje definice některých klíčových pojmů a je, do určité míry, vnitřně nekonzistentní. Chybějící definice a vnitřní nekonzistentnost zahrnují právě klíčové pojmy *použití síly* a *ozbrojený útok*. Vnitřní nekonzistentnost je tváří v tvář kybernetickým operacím spatřována také v zákazu použití síly (tedy jednoho způsobu realizace politické vůle), ale např. v povolení ekonomického nátlaku.[390] Vzhledem k povaze kybernetických operací může snadno dojít k amplifikaci vlivu těchto nekonzistentností,[391] které přitom nemusí při aplikaci na primárně kinetické prostředky boje činit zásadní potíže.

První prací, která vyčerpávajícím způsobem přistoupila k problematice aplikovatelnosti mezinárodního práva na kybernetické operace, byl Tallinnský manuál.[392] Tým odborníků, který na manuálu pracoval, postupoval s cílem zformulovat základní pravidla pro kybernetické operace tak, aby byla maximálně konsenzuální. Cílem tak byla konzervativní analogická aplikace existujících norem. U aplikace zápovědi obsažené v čl. 2 odst. 4 Charty OSN tým odborníků konstatoval, že kybernetická operace představuje hrozbu nebo použití síly ve chvíli, kdy je její rozsah a dopad analogicky srovna-

387 MSD (Nicaragua) 1986 op. cit., odst. 188.
388 Tamtéž, odst. 175.
389 Viz odpověď na druhou otázku v KOH, Harold Hongju, International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Ganecy Legal Conference Fr. Meade, MD, Sept. 18, 2012. *Harvard International Law Journal Online*, 2012, roč. 54, dostupné na http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.
390 Viz čl. 41 Charty OSN.
391 Viz LIN, Herbert. Cyber conflict and international humanitarian law. *International Review of the Red Cross,* 2012, roč. 94, č. 886, s. 524.
392 Tallinn Manual op. cit.

telný s dopadem nekybernetické (kinetické) operace, která by představovala hrozbu nebo použití síly.[393] Manuál tak klade důraz na tzv. kinetickou ekvivalenci[394] a soustředí se na následky operace. Kybernetická operace je protiprávní ve chvíli, kdy nahrazuje jinou protiprávní operaci – nerozhodují zde tedy použité prostředky. Tento přístup není zcela bez kontroverze, protože přesné hranice mezi jednotlivými kategoriemi nejsou konstruovány pouze na základě podobnosti mezi kinetickou a kybernetickou operací. Mohou být konstruovány i za použití jiných prostředků. Waxman předkládá čtyři způsoby, jakými je možné dosáhnout zásadního (a v zásadě podobného) vlivu na finanční systém jiné země – jedním z nich je zničení fyzické finanční infrastruktury leteckým úderem, další je regulatorní odstřižení, které znemožní provádět platby v zahraničních měnách, třetím je využití zpravodajských služeb pro distribuci podvržené měny a jiných finančních nástrojů na daném území a posledním je infiltrace systému a jeho narušení zevnitř prostřednictvím kybernetické operace.[395] Všechny případy v zásadě vedou k podobnému výsledku a striktní aplikace kinetické ekvivalence pro posouzení protiprávnosti tak rozhodně není jednoduchým úkolem.

V rámci manuálu jsou za účelem zhojení aspoň části nekonzistentností spatřovaných v dikci Charty OSN zavedeny následující premisy:[396]

- některé kybernetické operace nejsou použitím síly;[397]
- všechny ozbrojené útoky jsou automaticky použitím síly;[398]
- použití národních ozbrojených sil není nutnou podmínkou k překročení prahu použití síly.[399]

První premisa vychází ze specifické povahy kybernetických operací, kdy pouze některé budou obsahovat sekundární kinetický efekt. Jiné mohou spočívat pouze v odposlechu komunikace nebo šíření dezinformací a nemusí mít žádný kinetický efekt. Ty pak budou představovat donucovací

393 Tallinn Manual op. cit., s. 45 (pravidlo 11)
Hrozba použitím síly je konstruována podobně tamtéž – tamtéž, s. 52 (pravidlo 12).

394 CLARKE, Richard A. a Robert KNAKE. *Cyber War*, 2010, s. 178.
Srov. TUBBS, David, LUZWICK, Perry a Walter Gary SHARP. Technology and Law: The Evolution of Digital Warfare. *International Law Studies*, 2002, roč. 76, s. 7-20. S. 15.

395 Viz Waxman 2012 op. cit., s. 421-422.

396 Explicitně v Tallinn Manual op. cit., s. 47-48 (pravidlo 11, odst. 8).

397 Tallinn Manual op. cit., s. 46 (pravidlo 11, odst. 2-3).

398 Tamtéž, s. 46 (pravidlo 11, odst. 6).

399 Tamtéž, s. 46 (pravidlo 11, odst. 4).

akci, které ale není přímo způsobilá ohrozit územní celistvost – odehrává se v informační sféře, resp. sféře informační suverenity, která přímo neohrožuje území. Akce, které jsou ekonomickým či politickým donucováním by sice mohly být relevantní pro ustavení *kybernetické války* v rámci Clausewitzova konceptu, ale bez ohrožení územní celistvosti nemůže být operace hrozbou silou.[400] Manuál jako konkrétní příklad uvádí nekinetické kybernetické operace spadající do oblasti psychologické války.[401] O použití síly se v případě kinetických kybernetických operací může jednat ve chvíli, kdy je cílenému státu způsobena podstatná škoda. Může se jednat o ztráty na straně obyvatelstva nebo o škody na kritické infrastruktuře bez ohledu na její odvětví. Ve všech případech musí být naplněno kritérium rozsahu a efektu, resp. obě jeho složky – z rozsahu zápovědi použití síly jsou tak zřejmě vyloučeny akty *de minimis*. Z hlediska širšího dopadu manuálu bylo kritizováno, že se autoři soustředili primárně na otázku použití síly a nediskutovali související otázky – např. suverenitu a realizaci principu nevměšování se.[402] Právě hledání hranice mezi kybernetickými operacemi, které jsou užitím síly a které nikoli (ve vztahu ke kritériu rozsahu a efektu) by manuál mohl být návodnější.

Druhá premisa, která se objevuje v rámci manuálu, přímo navazuje na rozhodovací praxi Mezinárodního soudního dvora.[403] Ten v rámci rozhodnutí o činnosti vojenských a paravojenských jednotek v Nikaragui uvedl, že je nutné rozlišovat mezi nejzávažnějšími formami použití síly a mezi formami méně závažnými. Právě tyto nejzávažnější formy (v originále *„the most grave forms"*) představují ozbrojený útok. Rozlišení je zde důležité vzhledem k dikci čl. 51 Charty OSN, které je vykládáno tak, že právo na sebeobranu svědčí státu ve chvíli, kdy se stane cílem ozbrojeného útoku.[404] Z této premisy neplyne, že by kybernetická operace mohla být ozbrojeným útokem.

400 Tamtéž, s. 46 (pravidlo 11, odst. 3).

401 Tamtéž, s. 46 (pravidlo 11, odst. 3). Z toho dovozuji, že útoky bez sekundárního kinetického potenciálu je nutné považovat za nekinetické a z toho hlediska za neschopné stát se užitím síly dle mezinárodního práva.

402 FLECK, Dieter. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict & Security Law*. 2013, roč. 18, č. 2, s. 332-351. S. 346-347.

403 MSD (Nicaragua) 1986 op. cit., odst. 191.

404 Tamtéž, odst. 195.

Schopnost dosáhnout kybernetickou operací na nejzávažnější formu použití síly je spíše spekulativní. Hledání přesné odpovědi je problematické i vzhledem k tomu, že hranice mezi použitím síly a ozbrojeným útokem není příliš ostrá. Alternativní pohled na věc může představovat doktrína akumulace událostí.[405] Na základě tohoto přístupu je možné konstatovat, že v případě kontinuální kampaně, kdy jsou jednotlivé operace použitím síly, lze celou kampaň považovat za ozbrojený útok podle čl. 51 Charty OSN. Tato doktrína není ani zdaleka obecně přijímána,[406] nicméně kybernetické operace mohou být doménou, kde by její aplikace mohla vnést do související právních otázek trochu světla.

V rámci vztahu mezi doktrínou akumulace událostí a kybernetickými operacemi je nutné spatřovat dva základní problémy.[407] Jedním z nich je obecný problém s přičitatelností kybernetických operací. Aby bylo totiž možné na základě akumulace událostí dospět k závěru o existenci ozbrojeného útoku a aktivace práva na sebeobranu, je nutné jednotlivé operace vždy přičíst konkrétnímu státu. Jakkoli byla shora tato problematika relativizována do úrovně korelace cíle operace s politickými cíli konkrétního státu, zde je nutné postupovat výrazně opatrněji. Pro vyvození politické a diplomatické odpovědnosti nebo pro dovození konkrétní kampaně jako *kybernetické války* dle Clausewitze korelace možná dostačuje. Nicméně na konstatování existence ozbrojeného útoku, který je mezinárodně protiprávním jednáním, a zakotvení práva na sebeobranu v souladu s čl. 51 Charty OSN, nepostačuje. Zde je nutné trvat na kauzalitě. Druhým problémem v aplikaci

405 Angl. Accumulation of events, něm. Nadelstichtaktik.
Viz FEDER, Norman Menachem. Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack. *New York University Journal of International Law and Politics*, 1987, roč. 19, č. 2 s. 395-432. S. 415-418.

406 TAMS, Christian. The Use of Force against Terrorists. *The European Journal of International Law*, 2009, roč. 20, č. 2, s. 359-397. S. 370.
Také KRETZMER, David. The Inherent Right to Self-Defence and Proportionality in Jus ad Bellum. *The European Journal of International Law*, 2009, roč. 20, č. 2, s. 235-282. S. 263.

407 Vycházím z ROSCINI, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014. S. 110.
Roscini jmenuje tři, ale dva lze považovat za natolik zásadně provázané, že je není třeba dále rozdělovat.
Rosini zmiňuje (i) problém přičíst operaci konkrétnímu subjektu, (ii) problém provázat operace spolu navzájem jako součást strategicky orientované kampaně a (iii) problém s nutností, aby každá jednotlivá operace byla užitím síly ve smyslu čl. 2 odst. 4 Charty OSN.

akumulace událostí na kybernetické operace je požadavek, aby každá kybernetická operace, na jejímž základě dochází k akumulaci, byla sama o sobě užitím síly. V rámci části věnované diskuzi pojmu kybernetické války bylo uvedeno, že provedení kybernetické operace cílené na kompetentního protivníka vede k zásadnímu narušení schopnosti opakovat tutéž operaci. Kontinuální kampaň, v jejímž rámci budou všechny operace užitím síly, povede k zásadnímu vyprázdnění „zbraní" útočníka.

Třetí ze shora uvedených premis také vychází z rozhodovací praxe Mezinárodního soudního dvora. I za situace, kdy se operace neúčastní ozbrojené složky státu, je možné konstatovat, že se jedná o užití síly zakázané čl. 2 odst. 4 Charty OSN. Mezinárodní soudní dvůr v minulosti uvedl,[408] že v případě napomáhání paravojenským jednotkám na území cíle ve formě poskytování vybavení, financování, podpory a řízení jejich akcí je možné mluvit o použití síly.[409] V rámci kybernetických operací tak můžeme mluvit o poskytování sofistikovaného škodlivého kódu, o poskytování expertizy potřebné k jeho vytvoření nebo poskytnutí znalostí a zkušeností k jeho zavedení do cílového systému. V tuto chvíli nemusí nutně docházet k přímému použití ozbrojených sil útočníka, protože tuto činnost mohou vykonávat civilní pracovníci.

V důsledku vágních pojmů, ustavujících operaci jako použití síly nebo jako ozbrojený útok, a v důsledku velmi odlišného pohledu jednotlivých států na kybernetické operace autoři manuálu částečně rezignovali na objektivní posouzení kritérií. Autory byl zvolen tzv. policy-oriented přístup[410] jako přehlednější varianta – byť není pro právní posouzení výrazně jednodušší. Tento přístup mapuje faktory, které ovlivňují další postup napadeného státu[411] včetně pravděpodobnosti, že kybernetickou operaci vyhodnotí jako

408 MSD (Nicaragua) 1986 op. cit.

409 Jak bude nicméně uvedeno dále v textu, na stejném místě Mezinárodní soudní dvůr uvádí, že samotné poskytování finančních prostředků by bylo porušením principu nevměšování, ale nebylo by užitím síly podle čl. 2 odst. 4 Charty OSN.
Tamtéž, odst. 228.

410 SCHMITT, Michael N. The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski. In: CZOSSECK, Christian; Ottis, Rain; ZIOLKOWSKI, Katharina (eds.). *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, s. 311-317. ISBN 9789949904099. S. 316.

411 MCDOUGAL, Myres. Law as a Process of Decision: A Policy-Oriented Approach to Legal Study. *Natural Law Forum*, sv. 1, s. 53-72.

právně relevantní (tedy použití síly či ozbrojený útok). Otázka tedy není kladena s cílem získat objektivní odpověď, ale s cílem odhadnout, jaký názor na legálnost této operace má protivník.

Nejdůležitější faktory[412] pro toto kvalifikované rozhodnutí zahrnují tzv. Schmittova kritéria. Ta představují asistenční nástroje pro predikci dalšího postupu – nejedná se o normativní standardy.[413] Kritéria zahrnují:

- závažnost,
- okamžitý efekt,
- přímý efekt,
- míru invazivnosti,
- měřitelnost efektu,
- vojenský charakter,
- zapojení státu
- a domněnku legality.[414]

Ze všech předložených kritérií je jako nejdůležitější vnímána závažnost útoku, kde je možné zformulovat poměrně jasné *de minimis* pravidlo pro posouzení. Ve chvíli, kdy dojde k fyzickému zranění, úmrtí nebo škodě na majetku, budou státy více nakloněny možnosti uvažovat o kybernetické operaci jako o použití síly.[415] Ziolkowski k tomuto přístupu dodává, že dlouhodobé omezení funkčnosti kritické infrastruktury by mělo být také vnímání jako použití síly.[416]

Kritéria okamžitého a přímého efektu se soustředí zejména na rozlišování mezi ekonomickým donucováním a použitím síly zkoumáním kauzálního nexu spojujícího prvotní akci a její škodlivé následky. Zatímco v případě

412 Tato koncepce byla včetně části kritérií představena již v roce 1999. SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law,* 1999, roč. 37, č. 3, s. 885-938.

413 K diskuzi o povaze kritérií viz ZIOLKOWSKI, Katharina. Ius ad bellum in Cyberspace – Some Thoughts on the „Schmitt-Criteria" for the Use of Force. In: CZOSSECK, Christian; Ottis, Rain; ZIOLKOWSKI, Katharina (eds.). *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, s. 295-309. Také Schmitt 2012 op. cit., s. 316.

414 Tallinn Manual op. cit., s. 48-51 (pravidlo 11).

415 Nejedná se v tomto případě pouze o narušení suverenity, ale takováto akce je způsobilá vyvolat dostatečný mediální zájem a odpor veřejnosti k tomu, aby byly i opatrnější státy přinuceny k jednoznačným prohlášením.

416 Ziolkowski 2012, op. cit., s. 301-302.

ekonomického donucování se často jedná o spojení nepřímé, které není okamžitě zřejmě, přímé spojení mezi operací a následkem a okamžitá manifestace následku jsou charakteristické pro použití násilí. Kybernetické operace mající jasně provázanou příčinu s následkem,[417] tedy budou pravděpodobněji posuzovány jako užití síly. Toto kritérium úzce souvisí s povahou kybernetických operací. Škodlivý kód totiž může, ve spojení s provázaností cílené infrastruktury s dalšími zařízeními, mít neočekávané následky[418] – hypoteticky i měsíce po původní kybernetické operaci. Posouzení na základě tohoto kritéria tedy vyžaduje značné množství zpravodajských a technických informací o cíli operace.

Míra invazivnosti jako kritérium zohledňuje míru zabezpečení cílového systému. Využívá tím platící přímé úměry mezi mírou zabezpečení systému a mírou znepokojení v případě jeho narušení.[419] V případě zajištění určité standardizované míry zabezpečení kritické informační infrastruktury se dá předpokládat, že stát bude více inklinovat k možnosti vnímat kybernetickou operaci jako použití síly. Bude totiž přímo docházet k narušení explicitně (zákonem či jinak) chráněné hodnoty. Manuál přímo zmiňuje problematičnost[420] tohoto kritéria např. vzhledem ke značné invazivnosti kybernetických operací zaměřených na kybernetickou špionáž, která ale není jako taková zakázaná.

Kritérium měřitelnosti efektů souvisí se schopností kvantifikovat dopady kybernetické operace. V případě kybernetické operace, která směřuje vůči měkkým cílům, jako je veřejné mínění či důvěra ve stát, nebo u které není přímo jasné, co bylo jejím cílem, je problém změřit efekt. Efekt, který je jednoznačně měřitelný, např. počtem zraněných nebo konkrétní finanční ztrátou, bude s větší pravděpodobností označen za použití síly. Částečně to souvisí s politickou odvahou – rozhodnutí označit konkrétní operace jako užití síly má zásadní následky a nedostatečně kvantifikovatelný vliv tak pravděpodobnost pozitivní odpovědi zmenšuje.

417 Tallinn Manual op. cit., s. 49 (pravidlo 11, odst. 9).
418 Jensen 2003 op. cit.
419 Tamtéž.
420 Tallinn Manual op. cit., s. 50 (pravidlo 11, odst. 9).

Vojenský charakter představuje další kritérium, které je nutné vyhodnocovat. Jak bylo výše uvedeno, pro to, aby mohla být kybernetická operace považována za použití síly, není nezbytně nutné zapojení ozbrojených složek. *A contrario* se však domníváme, že v případě účasti ozbrojených složek se míra pravděpodobnosti, že napadený stát bude vnímat operaci jako použití síly, nezanedbatelně zvyšuje. Toto kritérium je ale nadáno stejným problémem jako výše uvedené kritérium míry invazivnosti – ozbrojené složky mohou být zapojeny do zpravodajských operací. Vojenský charakter operace také bude zřejmý spíše nepřímo – např. podle volby cíle nebo zvoleného postupu.

Zapojení státu navazuje na vojenský charakter, kdy má podobný smysl, ale volí odlišné prostředky. Zapojení státu tak může být poskytnutí sofistikovaného malwaru, poskytnutí výcviku nebo financování. Z hlediska použitelnosti tohoto kritéria pro posouzení, zdali je kybernetická operace užitím síly, je financování samotné irelevantní. Nedoprovázeno dalšími akcemi totiž nemůže být považováno za užití síly.[421] Aplikovatelnost tohoto kritéria je samozřejmě ovlivněna technickou realitou, tedy obecným problémem přičitatelnosti v rámci kyberprostoru.

Posledním navrženým kritériem je domněnka legality, která jediná představuje jistý zásah norem mezinárodního práva do struktury předložených kritérií. Mezinárodní právo totiž nezakazuje některé akce jako takové[422] – jedná se např. o metody psychologické války, špionáž či ekonomický nátlak. Pokud tedy bude kybernetická operace vnímána ve státě, který je cílem, optikou legálních operací, ochota označit kybernetickou operaci za užití síly bude převážně nízká.

Využití shora uvedených kritérií k právnímu posouzení operace je netriviální záležitost. Žádné z kritérií není za normální situace možné použít individuálně – operace nechávající za sebou několik zraněných a materiální škodu může být provedená tak, že znemožní provázání s konkrétním původcem. Stejně tak v případě výrazně odložené manifestace škodlivého kódu v řádu měsíců či let po provedení operace. Obecně je možné uvést, že některé druhy kybernetických operací mohou být porušením mezinárodněprávní zápovědi hrozby nebo použití síly. Tyto situace jsou nesmírně vzácné. Jak bylo

421 MSD (Nicaragua) 1986 op. cit., odst. 228.
422 Tallinn Manual op. cit., s. 51 (pravidlo 11, odst. 9).

uvedeno, měli jsme možnost je pozorovat v rámci experimentů, ale začíná se objevovat i jejich operační nasazení. Podobné situace se objevují v rámci scénářů, se kterými operují bezpečnostní složky po světě. Katastrofickým útokům na elektrickou síť nebo vesmírnou infrastrukturu[423] je věnována pozornost, byť často s upozorněním, že pravděpodobnost takového scénáře je malá. Vzhledem k možným následkům je ale aktivita států směřující k vyjasnění pravidel potřebná. Panující právní nejistota je částečně zhojena subjektivním přístupem, kdy se neposuzuje legálnost operace, ale pravděpodobnost, že ji cíl vyhodnotí jako nelegální. Náročnost tohoto rozhodnutí je enormní, protože vyžaduje velice přesné informace o povaze operace, použitých prostředcích a také o operačních a organizačních opatřeních cíle operace. Zformulování názoru na problematiku tak, aby bylo možné v rámci praxe státu provádějícího kybernetické operace možné uzavřít o jeho legalitě, by přispělo ke zvýšení právní jistoty. Kybernetické operace jsou realitou mezinárodních vztahů a narovnání prostředí, ve kterém se odehrávají, je jistě žádoucí.

Další část textu se po diskuzích o aplikaci *ius ad bellum* věnuje aplikaci *ius in bello*, kde také čelíme novým otázkám – nikoli na úrovni aplikovatelnosti právního rámce, ale na úrovni způsobu jeho aplikace.

423 Viz LIVINGSTONE, David a Patricia LEWIS. *Space, the Final Frontier for Cybersecurity?* Chatham House, 2016. Dostupné z: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity

12 TECHNOLOGICKÁ VÝZVA HUMANITÁRNÍMU PRÁVU

12.1 Martensova klauzule

Všechny právní normy nezbytně zastarávají. Jak podotkl Harold Koh, současný rozvoj kybernetických operací není první případ situace, kdy se technologická realita změnila a mezinárodní právo se s tím musí vypořádat.[424] Normy mezinárodního práva veřejného jsou nicméně obecně nadány nízkou dynamikou – a i když právo *„nepochybně předvídá technologický vývoj a předpovídá, že existující pravidla lze na tento vývoj vztáhnout"*[425] a *„staré právo umožňuje odpovídat na nové otázky"*,[426] nejsou tyto odpovědi vždy bez diskuzí a okamžitě k dispozici. A také není vždy jasné, jakým způsobem se stará pravidla na nový kontext vztahují. Určitou míru dynamizace umožňuje tzv. Martensova klauzule. Jak podotkl Mezinárodní soudní dvůr ve stanovisku k legálnosti hrozby nebo použití jaderných zbraní,[427] klauzule se stala *„efektivním prostředkem k adresování rychlé evoluce vojenských technologií."*[428] Přesná povaha Martensovy klauzule a přesný způsob, jakým umožňuje zvyšovat dynamiku jinak velmi statických norem, je však stále předmětem diskuze.

Martensova klauzule nese jméno Friedricha Fromholda Martense – nebo také Fjodora Fjodoroviče Martense – vyslance carského Ruska na kongresu v Haagu v roce 1899. Dle dostupných pramenů klauzule neměla být pojistkou pro případ technologického vývoje, ale vznikla v podstatě náhodou jako snaha urovnat spor, který v rámci vyjednávání o znění Haagských smluv vypuknul mezi menšími evropskými zeměmi (pod vedením Belgie) a jejich

424 Srov. odpověď na druhou otázku v rámci Koh 2012 op. cit.

425 Tamtéž.

426 KODAR, Erki. Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I. In: LIIVOJA, Rain a Andres SAUMETS (eds.). *The Law of Armed Conflict: Historical and Contemporary Perspectives*. Tartu University Press: Tartu, 2012. S. 107.

427 V české literatuře shrnuto v POTOČNÝ, Miroslav. Otázka legality hrozby nebo použití jaderných zbraní. *Mezinárodní vztahy*, 1999, roč. 34, č. 1, s. 97-105.

428 MSD (Nuclear Weapons) 1996 op. cit., odst. 78. Shodně Sandoz 1987 op. cit., odst. 55, kde se uvádí: *„it should be seen as a dynamic factor proclaiming the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology"*.

většími sousedy.[429] V rámci jednání vyžadovala Belgie neomezené právo na odpor pro obyvatele okupovaného území.[430] Martensovo vystoupení, jehož část byla nakonec zařazena do preambule sjednané smlouvy, vznikající spor zažehnalo a přispělo ke zdárnému ukončení jednání.

Původně se tak Martensova klauzule objevila v rámci preambule k Haagské Úmluvě o zákonech a obyčejích války pozemní z roku 1899 v následujícím znění: *„Dokud není vydán kompletnější kodex válečného práva, Vysoké smluvní strany se domnívají, že je správné vyhlásit, že v případech, na něž nedopadá tato regulace jimi přijatá, obyvatelé a válčící strany zůstávají pod ochranou mezinárodního práva jako důsledku zvyků zavedených mezi civilizovanými národy, pravidel lidskosti a diktátu veřejného svědomí.“*[431]

Dnes je klauzule chápána jako účinná pojistka pro případ technologického vývoje,[432] který je možné v rámci vojenských technologií pozorovat více, než kde jinde. Kromě toho ale Martensova klauzule představuje hodnotový rámec pozemní války a její umístění v rámci preambule lze vnímat jako jistou deklaraci.[433]

Rozměr Haagského práva, tedy práva válečného, pak byl definitivně překročen zakomponováním klauzule do práva Ženevského, humanitárního, v rámci čl. 1 odst. 2 Dodatkového protokolu I z roku 1977 k Ženevským konvencím z roku 1949 a v rámci preambule Dodatkového protokolu II z roku 1977 k Ženevským konvencím z roku 1949.

---

429 PUSTOGAROV, Vladimir Vasilievich. *Fyodor Fyodorovich Martens (1845-1909) – a humanist of modern times*. Dostupné z: https://www.icrc.org/eng/resources/documents/article/other/57jn52.htm

430 Dnes je regulováno v rámci ŽK a ani zdaleka se nejedná o právo absolutní, nicméně základní ochrana je účastníkům povstání na okupovaném území přiznávána.

431 Preambule, překlad autor. *Laws of War: Laws and Customs of War on Land (Hague II); July 29, 1899*. Dostupné z: http://avalon.law.yale.edu/19th_century/hague02.asp.

432 MSD (Nuclear Weapons) 1996 op. cit., odst. 78. Také SANDOZ, Yves, SWINARSKI, Christophe a Bruno ZIMMERMANN (eds.). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: International Committee of the Red Cross, 1987. Dostupné z: http://www.loc.gov/rr/frd/Military_Law/RC_commentary-1977.html. Odst. 55.

433 Bývá tak akcentován spíše její silný rétorický význam nebo etická normativita, který jde ruku v ruce se značnou vágností z hlediska právního významu.
Srov. také MERON, Theodor. The Martens Clause, Principles of Humanity, and Dictates of Public Conscience. *The American Journal of International Law*, 2000, roč. 94, č. 1, s. 79.

Dodatkový protokol II obsahuje formulaci, že Vysoké smluvní strany připomínají, že *„v případech, které nejsou upraveny platným právem, zůstává lidská osobnost pod ochranou zásad humánnosti a požadavků společenského svědomí.“*[434]

Dodatkový protokol I pak jako jednu ze všeobecných zásad jmenuje, že *„[v] případech, které neupravuje tento Protokol nebo jiné mezinárodní dohody, zůstávají civilní osoby a kombatanti pod ochranou a v rámci působnosti zásad mezinárodního práva vyplývajících z ustálených obyčejů, ze zásad lidskosti a z požadavků společenského svědomí.“*[435]

V té době byla klauzule částečně chápána jako součást obyčejového práva, k čemuž přispěly Norimberské procesy. V jejich rámci byla opuštěna pozice Martensovy klauzule jako deklarace nadané symbolickým významem a byla přijata její pozice generální klauzule mezinárodního práva.[436]

Bohužel přesný vliv Martensovy klauzule jako obecného principu mezinárodního práva je poměrně nejasný, resp. je předmětem mnoha různých výkladů od velmi restriktivních po extenzivní. Pozorujeme tedy snahy klauzuli maximálně marginalizovat, např. tvrzením, že se kompletní úpravou v rámci Ženevských konvencí stala obsoletní,[437] či radikální snahy pouze na jejím základě zakázat využívání semi-autonomních a autonomních bojových prostředků.[438] První extrém klauzuli zcela vylučuje z role byť i jen interpretačního vodítka, zatímco druhý extrém ji povyšuje na úroveň nezávislého pramene mezinárodního práva. Většina existujících výkladů však stojí někde mezi těmito dvěma vyhraněnými pozicemi.

---

434 Preambule Dodatkového protokolu II

435 Článek 1, odst. 2 Dodatkového protokolu I

436 *Krupp et al. US Military Tribunal Nuremberg, Judgment of 31 July 1948*. Dostupné z: http://werle.rewi.hu-berlin.de/KRUPP-Case%20Judgment.pdf. S. 14-15.
Na zásady humánnosti se odvolává i rozhodnutí Altstotter - The United Nations War Crimes Commission. *Law Reports of Trials of War Criminals, Volume VI*. His Majesty's Stationery Office: London, 1948. Dostupné z: http://www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-6.pdf. S. 58.
Také MSD (Nuclear Weapons) 1996 op. cit., odst. 78.

437 *Letter dated 19 June 1995 from the Ambassador of the Russian Federation, together with Written Comments of the Goverenment of the Russian Federation*. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/8796.pdf

438 Human Rights Watch. *Loing Humanity: The Case against Killer Robots*. 2012. Dostupné z: http://reliefweb.int/sites/reliefweb.int/files/resources/Losing%20Humanity%20The%20Case%20Against%20Killer%20Robots.pdf. Ostrou výtku tomuto chápání adresoval např. EVANS, Tyler D. At War with the Robots: Autonomous Weapon Systems and the Martens Clause. *Hofstra Law Review*, 2013, roč. 41, č. 3, s. 697-733. Opačně také Meron 2000 op. cit., s. 88.

Další pozice zahrnuje označení Martensovy klauzule jako korektivu k principu vycházejícímu z případu *Lotus*, kde soud uvedl, že suverénní stát může konat jakýmkoli způsobem, který nenarušuje explicitní zákaz. Martensova klauzule interpretovaná tímto způsobem zakládá existenci situací, kdy nezakázané jednání může být protiprávní. Funguje tak jako zápověď *a contrario* argumentu – co není zakázáno, nemusí být nutně dovoleno.[439] V tomto duchu nemá klauzule žádným způsobem určovat, jak jsou pravidla vytvářena, ale pouze připomínat existující obyčeje na pozadí smluvního práva.[440] Platí, že neexistuje a nemůže existovat kompletní a definitivní úprava v rámci jakékoli mezinárodní smlouvy[441] – vzhledem k nepřítomnosti státům nadřazeného normotvůrce budou vždy vznikat časové prodlevy mezi technologickým vývojem a reakcí práva. Tento pohled na Martensovu klauzuli tak akcentuje její pragmatickou povahu, spíše než přirozenoprávní rétoriku.[442] Obecně lze říci, že restriktivní interpretace kladou důraz na právní jistotu, která by byla moralistickými argumenty vznášenými prostřednictvím klauzule, narušována.[443] Restriktivní výklad je dodnes velmi populární, i když poválečný vývoj ho z velké části vyvrací – Norimberský tribunál totiž využíval Martensovy klauzule poměrně extenzivně.[444]

Extenzivněji lze využít Martensovy klauzule jako interpretační pomůcky – Cassese tvrdí, že klauzule umožňuje soudu posoudit operace jako protiprávní ve chvíli, kdy by rozšíření v důsledku konstatování legálnosti vedlo k nehumánním následkům.[445] Podobně se vyjádřil i Mezinárodní trestní tribunál pro bývalou Jugoslávii, když uvedl, že *opinio juris sive neccesitas*[446] může v některých situacích hrát výrazně větší roli než praxe jednotlivých států,

439 Srov. CASSESE, Antonio. The Martens Clause. Half a Loaf or Simply Pie in the Sky? *European Journal of International* Law, 2000, roč. 11, č. 1, s. 189. Také Meron 2000 op. cit., s. 81.

440 FLECK, Dieter (ed.). *The Handbook of Humanitarian Law in Armed Conflicts*. Oxford University Press: Oxford/New York, 1995. S. 28. Srov. Meron 2000 op. cit., s. 87-88.

441 Sandoz 1987 op. cit., odst. 55.

442 SALTER, Michael. Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 3, s. 405.

443 Salter 2012 op. cit., s. 410.

444 Tamtéž, s. 412.

445 Uvádí tak, že klauzule rozhodně nekonstruuje dva nové prameny mezinárodního práva, ale umožňuje k jejich diktátu přihlédnout. Viz Cassese, 2000 op. cit., s. 211.

446 Formulované právě zásadami lidskosti.

která může chybět nebo být nekonzistentní.[447] Toto pojetí Martensovy klauzule tak akcentuje (do určité míry) soudní aktivismus – soudy mají jinou motivaci než státy a jsou ochotnější k postupné humanizaci konfliktů.[448] Salter jde ještě dál a sahá k historickému výkladu – pokud byla Martensova klauzule schopna vyřešit na konci 19. století, jistě nebyla pouze výkladovým vodítkem. Představovala proto, a dodnes představuje, nezávislou normu,[449] která v kombinaci s existujícím právním rámcem umožňuje jeho analogickou aplikaci na nové situace. V obou případech tyto extenzivní výklady vedou k jednodušší kvazi-legislativní povaze soudního výkladu a k větší flexibilitě mezinárodněprávních norem. K tomu ostatně přispěl i vývoj ve společnosti – jak uvádí Meron, tento silný tah směrem k normativitě klauzule by nebyl možný bez dramaticky rostoucího vlivu médií, nevládních organizací či Mezinárodního výboru Červeného kříže.

V souvislosti s Martensovou klauzulí je často citované stanovisko Mezinárodního soudního dvora k legálnosti hrozby nebo použití jaderných zbraní. Soud se v něm sice přímo nezaobíral povahou Martensovy klauzule, ale písemná i ústní podání jednotlivých států či odlišná stanoviska jednotlivých soudců se často věnovala povaze Martensovy klauzule ve vztahu k dynamizaci mezinárodního práva.

Ruská federace ve svém podání označila Martensovu klauzuli za obsolentní vzhledem ke kompletnímu zachycení práva ozbrojeného konfliktu v rámci konvencí z roku 1949 a jejich dodatků z roku 1977.[450] Za zcela nespornou tak přijala premisu možnosti kompletní úpravy problematiky v rámci smluvního práva. Tím došlo k flagrantnímu opomenutí zjevné kontinuity Martensovy klauzule. Hodnotový rámec, který klauzule představovala v původním Haagském právu, pokračuje, tentokrát však jako inherentní součást smluvního práva Ženevského ve výše uvedeném čl. 1 odst. 2 Dodatkového protokolu I.

Spojené království uvedlo, že samotný fakt absence specifické smlouvy zakazující hrozbu nebo použití jaderných zbraní nečiní takové jednání

447 Mezinárodní trestní tribunál pro bývalou Jugoslávii. *Kupreškič et al. – Judgment of 14 january 2000*. Dostupné z: http://www.icty.org/x/cases/kupreskic/tjug/en/kup-tj000114e.pdf. Odst. 527. Opačně srov. MSD (Nicaragua) 1986 op. cit., odst. 184.

448 Srov. Meron 2000 op. cit., s. 89.

449 Viz Salter 2012 op. cit., s. 421-432.

450 Dopis (Rusko) 1995 op. cit., s. 13.

automaticky dovoleným, nicméně učinilo tak způsobem marginalizujícím klauzuli. Uvedlo totiž, že ve chvíli absence jasného zákazového pravidla musí být konání státu povolené.[451] Toto doplnilo argumentem, že ani přesto nemá suverénní stát možnost vybrat si jakýkoli způsob, kterým své vojenské operace povede.[452] Neexistence specifické smlouvy o použití jaderných zbraní dle tohoto názoru neznamená, že je možné je legálně použít, ale Martensova klauzule sama o sobě není schopná založit jejich zákaz, resp. ilegální povahu jejich použití.[453]

Za poměrně zajímavý materiál je nutné považovat písemné podání ostrovního státu Nauru. Podání předkládalo argument, že v klauzuli obsažený odkaz na veřejné svědomí znamená mimo jiné možnost vyjádřit se k legalitě či ilegalitě specifického bojového prostředku osobám nebo organizacím, které jsou vysoce kvalifikované vyjadřovat se na téma práva ozbrojeného konfliktu.[454] Zároveň ale stanovuje jako podmínku, že by tyto osoby či organizace neměly být přímo afiliované ke konkrétním vládám.

Mezinárodní soudní dvůr nakonec ve svém stanovisku pouze lakonicky poznamenal, že Martensova klauzule se stala efektivním nástrojem, který umožňuje postavit se rychlému nástupu nových vojenských technologií. Martensovu klauzuli pak využil jako výkladové vodítko[455] a také k potlačení *a contrario* argumentu.[456]

Z hlediska výkladu Martensovy klauzule byla zajímavá převážně disentní stanoviska soudců Koromy, Weeramantry a Shahabuddena, která mu věnovala více pozornosti.

451 *Letter dated 16 June 1995 from the Legal Adviser to the Foreign and Commonwealth Office of the United Kingdom of Great Britain and Nothern Ireland, together with Written Comments of the United Kingdom*. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/8802.pdf. S. 21.
Dopis se v tomto argumentu odvolával zejména na MSD (Nicaragua) 1986 op. cit., odst. 269.

452 Čl. 35, odst. 1 Dodatkového protokolu I.

453 Dopis (Spojené království) 1995 op. cit., odstavec 3. 58. Implicitně také obsaženo v odstavci 4. 2.

454 *Letter dated 15 June 1995 from Counsel Appointed by Nauru, together with Written Comments of the Government of Nauru*. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/8794.pdf. S. 8.

455 MSD (Nuclear Weapons) 1996 op. cit., odst. 78.

456 MSD (Nuclear Weapons) 1996 op. cit., odst. 84.
Srov. Dissenting opinion of Judge Shahabudden. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/7519.pdf. S. 183.

Soudce Koroma se ve svém stanovisku k Martenově klauzuli vyslovil s důrazem na její kontinuitu v právu (tedy i po výskytu v úmluvách z roku 1899 a 1907) a přisoudil jí pozici zachycení principů, na kterých mezinárodní právo stojí. Zároveň opatrně kritizoval většinové rozhodnutí v jeho snaze hledat v právu explicitní zákaz, namísto konstatování zákazu implicitně plynoucího z dikce Martensovy klauzule. Tuto zbytečnou cestu za explicitními zákazy metod boje porušujících principy mezinárodního práva označil za extrémní formu pozitivismu.[457]

Soudce Weeramantry zmínil, že zatímco původně sloužila Martensova klauzule k výše uvedenému překlenutí rozdílných názorů ohledně povahy hnutí odporu na okupovaném území, je nyní aplikovatelná i mimo tuto oblast a tedy na celé právo humanitární.[458] Je tak součástí korpusu současného mezinárodního práva.[459] Ve smyslu písemného podání Nauru pak konstatoval, že bez ohledu na povahu Martensovy klauzule obecně byla její působnost na oblast jaderných zbraní dokázána konstantním zájmem mezinárodního společenství o tuto otázku a častými vyjádřeními ve vztahu k přípustnosti hrozby použitím nebo použití těchto zbraní hromadného ničení.[460]

Soudce Shahabudden kladl důraz na výše uvedenou normativní povahu Martensovy klauzule a uvedl, že je samostatně aplikovatelná. Ze znění klauzule v její původní podobě v roce 1899 dovozuje snahu řešit jejím prostřednictvím mezery v mezinárodním právu.[461] Připomíná pak závěr Seana McBrida, že Martensova klauzule poskytla mezinárodnímu právu dynamiku jinak nedosažitelnou.[462] O tu pak není možné mezinárodní právo ochudit pod žádnou záminkou.

Martensova klauzule tak dle našeho názoru může být chápána jako projev přítomnosti přirozeného práva v právu mezinárodním. Positivistická interpretace mezinárodního práva stanovuje, že státy, které nesouhlasí se svojí vázaností určitým pravidlem, jím nejsou vázány. Zůstávají tím mimo rozsah

457 *Dissenting opinion of Judge Koroma*. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/7523.pdf. S. 353.
458 Stanovisko (Koroma) op. cit., s. 261.
459 Dissenting opinion of Judge Weeramantry. Mezinárodní soudní dvůr. Dostupné z: http://www.icj-cij.org/docket/files/95/7521.pdf. S. 264.
460 Stanovisko (Weeramantry) op. cit., s. 265-266.
461 Stanovisko (Shahabudden) op. cit., s. 183.
462 Stanovisko (Shahabudden) op. cit., s. 183.

jeho aplikace. Podřízení se určité normě tak představuje svobodné rozhodnutí státu, ke kterému ho, při chybějícím sankčním mechanismu mezinárodního práva, nemůže nutit žádná vnější síla. Jedná se o právo, jehož působnost je přímo založená souhlasem. Možnost výhrady vůči zvykovému právu existuje.

Státy nejvíce zasažené zakotvením obyčejového charakteru určité normy mohou zabránit tomu, aby se z normy de lege ferenda stala norma de lege lata. V rámci právní regulace jaderných zbraní by tak byla nejdůležitější praxe států, které jsou příslušníky tzv. jaderného klubu. Státy se mohou nejenom rozhodnout podřídit smluvnímu právu, ale mohou se, v případě, že prokáží, že by se jich norma zásadním způsobem dotkla, vymezit i vůči zakotvení obyčejového pravidla.[463] Na vývoj práva v oblasti kybernetických operací tak budou mít vliv technologicky nejrozvinutější armády světa. Zatímco členství v tzv. jaderném klubu je víceméně veřejnou záležitostí, resp. dá se dovozovat, kybernetické ofenzivní schopnosti podléhají zásadním způsobem vysoké míře utajení.

Z politického hlediska registrujeme již zmíněnou odlišnou vůli v přístupu k této otázce na úrovni NATO a vůči nim politicky či vojensky se vymezujících subjektů, jako je Čína, Rusko, Irán nebo Severní Korea.[464]

Přirozenoprávní přístup v tuto chvíli zavazuje všechny obyvatele a všechny státy a jedná se tak o nekonsensuální koncept založený na prevalenci práv a spravedlnosti. Je otázka, nakolik je tento koncept ještě schopný přežít a ovlivňovat interpretaci a aplikaci norem mezinárodního práva. Při pohledu optikou přirozeného mezinárodního práva slouží právo spravedlnosti a humanitě, právě ve smyslu Martensovy klauzule. Neslouží primárně moci a mocenským zájmům. Akceptace pozitivněprávního přístupu a vyloučení normativní povahy Martensovy klauzule by nás tak přiblížilo realistickému pojetí mezinárodního práva, které je formováno právě vůlí státu, resp. států relevantních z hlediska vojenské moci či politického vlivu.

463 Pustogarov 1996 op. cit.

464 Srov. Meron 2000 op. cit., s. 88.
Důležitou součástí práva válečného práva i práva ozbrojeného konfliktu je vzájemnost a zde je tedy nutné připomenout její současnou neexistenci.

Martensova klauzule posloužila jako tiché memento přirozenoprávního přístupu v rámci řízení o ilegalitě jaderných zbraní a její normativní povaha byla, dle mého, přesvědčivě zakotvena. Z hlediska České republiky se tak jedná o koncept, který by měla aktivně podporovat, jelikož tím nedochází k vyřazení menších[465] států z účasti na rozhodování o vývoji práva ozbrojeného konfliktu. Při zdůraznění přirozenoprávního přístupu k normativitě Martensovy klauzule je nám poskytnut hodnotový rámec, který nám umožní vyrovnat se s technologickým pokrokem.

12.2 Rozlišování při použití kybernetických prostředků

Jedním ze základních principů mezinárodního humanitárního práva, a to jak v rámci smluv, tak v rámci obyčejů, je princip rozlišování (*distinction*). Mezinárodní soudní dvůr formuloval v rámci svého již zmíněného stanoviska k otázce legality hrozby nebo použití jaderných zbraní hlavní principy mezinárodního práva jako zahrnující rozlišování mezi kombatanty a nekombatanty, ochranu civilní populace a civilních objektů a zákaz způsobovat komtabantům nadměrné utrpení. Mezinárodní soudní dvůr uvedl, že státy nikdy nesmí cílit své útoky na civilisty a nesmí používat zbraně, které nejsou schopné rozlišit mezi civilními a vojenskými cíli.[466] Touto optikou je tak nutné chápat princip rozlišování v rámci dnešního mezinárodního humanitárního práva.

Možnost aplikace na moderní technologie, resp. schopnost přizpůsobit se moderním technologiím, je zajištěna v čl. 1 odst. 2 Dodatkového protokolu I. Tato norma je podpořena zněním článku 36 Dodatkového protokolu I. Ten stanovuje pro smluvní strany povinnost určit při studiu, vývoji nebo zavádění nových druhů zbraní, prostředků nebo způsobů vedení války, zda jejich použití není za některých okolností zakázáno pravidly vedení války. I výše zmíněné stanovisko Mezinárodního soudního dvora zdůrazňovalo nezbytnost použít existující pravidla na všechny formy vedení války a na všechny druhy zbraní.[467] Bylo by proti smyslu této úpravy brát ohled na to, jestli jsou nebo nejsou explicitně zakotvené.

465 V tomto kontextu spíše méně relevantních.
466 MSD (Nuclear Weapons) 1996 op. cit., odst. 78.
467 MSD (Nuclear Weapons) 1996 op. cit., odst. 86.

Princip rozlišování je přímo formulován v čl. 48 Dodatkového protokolu I. V první části tohoto článku je uveden příkaz stranám konfliktu k rozlišování mezi civilní populací a kombatanty a mezi civilními objekty a vojenskými cíli, a to za všech okolností. Ve druhé navazující části pak přikazuje, aby byly vojenské operace vedeny pouze proti vojenským cílům. Civilní populace a civilní objekty tak musí být v rámci ozbrojeného konfliktu rozlišovány a ochraňovány. Legitimním cílem válčících stran je totiž primárně oslabení vojenské moci protivníka. Ochranu civilní populace je tedy nutné chápat jako neoddělitelnou od příkazu rozlišovat.[468]

Až do 1. světové války nebyl přímý příkaz k rozlišování a ochraně zcela nezbytný. Civilní populace se zřídkakdy dostávala do přímého kontaktu s vojenskými operacemi v rámci bojových zón, resp. dostávala se s nimi do kontaktu pouze, pokud byla lokalizována v bojové oblasti.[469] Konflikt, od jehož počátku již uplynulo více než století, však přinesl zásadní změnu v podobě nasazení dělostřelectva s větším dostřelem a leteckého bombardování. Tyto změny se prohlubovaly v rámci 2. světové války, která navíc k vývoji přispěla dalšími změnami. Vojenské operace začaly být cílené přímo na obyvatelstvo v důsledku změny prozatímního chápání konfliktu s nástupem totální války. K vedení totální války stát nezbytně nutné potřeboval zmobilizovat všechny své zdroje, ať už materiální nebo personální.[470] Součástí zlomení vojenské moci protivníka se tak stalo nejen přímé oslabení vojenských sil protivníka, ale i narušení jeho schopnosti udržovat bojové operace a zlomení jeho vůle pokračovat v boji. V důsledku toho se operace zaměřovaly i na civilní obyvatelstvo, na výrobní schopnosti státu a na celkovou vůli vést konflikt. Válka přestala rozlišovat. Právě smlouvy přijaté v období po roce 1945 směřují proti návratu totální války, tedy proti vedení konfliktu, ve kterém by bojující strany nerozlišovaly mezi civilisty a kombatanty.

Na rozdíl od některých vágních pojmů předchozí části věnované *ius ad bello* máme k dispozici definiční ustanovení obsahující vymezení civilistů a civilního obyvatelstva.

468 Sandoz 1987 op. cit, odst. 1911.
469 Sandoz 1987 op. cit, odst. 1865.
470 Viz TOWNSHEND, Charles (ed.). The Oxford History of Modern War. Oxford: Oxford University Press, 2000. S. 139-141.

Čl. 50 odst. 1 Dodatkového protokolu I definuje civilistu za pomocí negativního vymezení tak, že civilistou je každá osoba, která není

- příslušníkem ozbrojených stran konfliktu nebo příslušníkem milicí a dobrovolnických jednotek v těchto ozbrojených silách;[471]
- příslušníkem jiných milic nebo dobrovolnických sborů, včetně členů organizovaného hnutí odporu, kteří náležejí ke straně konfliktu a operují na vlastním území i mimo něj. Tyto milice nebo dobrovolnické sbory musí mít ve svém čele osobu odpovědnou za své podřízení, dále musí mít pevný rozeznávací znak viditelný na dálku, nosit zbraně otevřeně a dodržovat při svých akcích zákony a obyčeje.[472]
- příslušníkem pravidelných ozbrojených sil hlásících se k vládě nebo moci neuznané mocností držící zajatce;[473]
- obyvatelem neobsazeného území, který se při příchodu nepřítele z vlastního popudu chopí zbraně, aby s ní bojoval. Podmínkou je, že bude otevřeně nosit zbraně a zachovávat zákony a obyčeje;[474]
- členem ozbrojených složek strany konfliktu, který je přímo pod velením osoby zodpovědné straně konfliktu za jednání svých podřízených. Toto platí, i pokud nejsou uznání protivníkem.[475]

Civilní obyvatelstvo se pak skládá z osob, které jsou civilisty.[476] Je nutné upozornit, že civilní obyvatelstvo nemůže svůj civilní charakter (a tím pádem ani ochranu) ztratit, pokud se v jeho středu pohybují osoby, které nejsou civilisty.[477] Obecnou ochranu požívá civilní populace před nebezpečím plynoucím z vojenských operací.[478] Zároveň nesmí být civilní populace ani jednotliví civilisté cíleni použitím síly, které primárně míří k vyvolání strachu mezi civilním obyvatelstvem.[479]

471 Článek 4, odst. 1, část 1 Třetí Ženevské úmluvy o ochraně obětí války.
472 Článek 4, odst. 1, část 2 Třetí Ženevské úmluvy o ochraně obětí války.
473 Článek 4, odst. 1, část 3 Třetí Ženevské úmluvy o ochraně obětí války.
474 Článek 4, odst. 1, část 6 Třetí Ženevské úmluvy o ochraně obětí války.
475 Článek 43, odst. 1 Dodatkového protokolu I.
476 Článek 50, odst. 2 Dodatkového protokolu I.
477 Článek 50, odst. 3 Dodatkového protokolu I.
478 Článek 51, odst. 1 Dodatkového protokolu I.
479 Článek 51, odst. 2 Dodatkového protokolu I.

Tato ochrana trvá, dokud se civilisté nezapojí do boje. Ve chvíli, kdy se do boje přímo zapojí, ztrácejí ochrany poskytovanou jim právem. Ztráta ochrany však trvá pouze po dobu přímého zapojení do boje.[480]

Princip rozlišování a ochrany civilní populace je přímo posílen stanovením konkrétních podmínek pro vojenské operace. Nerozlišující vojenské operace jsou obecně zakázané.[481] Nerozlišující je obecně chápáno jako necílené na specifický vojenský cíl[482] nebo používající metody, které nemohou být na konkrétní vojenský cíl zaměřeny.[483] Zakázáno je i používání prostředků, jejichž účinek nemůže být omezen a v každém případě tak zasahuje vojenské cíle i civilní osoby nebo civilní objekty.[484] Přímo zakázané jsou útoky, u nichž se dá očekávat, že mohou způsobit ztráty na životech civilních osob, škodu civilním budovám nebo kombinaci obojího, pokud by ve svých dopadech převyšovaly předpokládanou konkrétní a přímou vojenskou výhodu.[485]

Útoky mají být striktně omezeny na vojenské cíle, které jsou chápány jako objekty, z jejichž polohy, účelu nebo použití vyplývá efektivní přispění k nepřátelskému vojenskému snažení a jejichž částečné nebo celkové zničení nebo vyřazení z provozu vede k získání specifické vojenské výhody.[486]

Nakonec je *expressis verbis* zakázáno útočit na objekty, které zadržují nebezpečné přírodní síly, např. přehrady a jaderné elektrárny. Tento zákaz platí i ve chvíli, kdy je tento objekt jinak možné považovat za vojenský cíl, pokud by jeho zničení mohlo způsobit uvolnění nebezpečných sil a následné ztráty na životech civilní populace.[487] Z dikce tak dle našeho názoru vyplývá, že pokud je objekt zadržující nebezpečné přírodní síly vyhodnocen jako vojenský cíl a jeho zničení nezpůsobí ztráty na životech civilní populace, bude

480 Článek 51, odst. 3 Dodatkového protokolu I. Toto pravidlo je dnes kritizováno, protože neumožňuje zbavení ochrany ve chvíli, kdy dochází činností civilisty ke zvyšování bojové kapacity (např. poskytnutím specializovaného výcviku) nebo k udržování bojové kapacity (např. opravou vybavení) – viz SCHMITT, Michael. Military Necessity and Humanity. *Virginia Journal of International Law*, 2010, roč. 50, č. 4, s. 833.

481 Článek 51, odst. 4 Dodatkového protokolu I.

482 Článek 51, odst. 4, písm. a) Dodatkového protokolu I.

483 Článek 51, odst. 4, písm. b) Dodatkového protokolu I.

484 Článek 51, odst. 4, písm. c) Dodatkového protokolu I.

485 Článek 51, odst. 5 Dodatkového protokolu I.

486 Článek 52, odst. 2 Dodatkového protokolu I.

487 Článek 56, odst. 1 Dodatkového protokolu I.

možné jej cílit v rámci tzv. A2/AD[488] operací. De lege lata je tak legální vést kybernetickou operaci proti SCADA systému přehrady za účelem vypuštění vody do oblasti strategického významu za účelem získání vojenské výhody.

Obecně princip rozlišování nesměřuje ke stavu, kdy nikdo z civilistů neutrpí zranění, ale míří spíše k minimalizaci dopadu vojenských operací na civilní obyvatelstvo. Určitá míra škod je samozřejmě nevyhnutelná.[489] Je tak zakázáno plánovat, přikázat nebo provést[490] útok na vojenský cíl, u kterého lze očekávat vedlejší škody, které budou excesivně disproporcionální ve vztahu k očekávané konkrétní a přímé vojenské výhodě, kterou by bylo možné operací získat.[491] Tento princip, někdy označovaný také jako princip proporcionality, je mimo jiné i obyčejem.[492]

Mezinárodní humanitární právo se žádným způsobem nevyjadřuje k proporcionalitě lidských ztrát v rámci kombatantů stran konfliktu nebo při porovnávání poškození, jaké utrpěli jejich vojenské objekty. Princip proporcionality není chápán jako směřující k omezení lidských a materiálních ztrát stran konfliktu na podobnou míru. Při útoku proti vojenským cílům protivníka neexistuje limitace použití síly, ale existuje právě ohled na vedlejší škody způsobené civilní populaci.[493] Ne každá nepříjemnost způsobená civilní populaci je relevantní pro účely rozlišování, ochrany a proporcionality. Nedostatky v dodávkách jídla nebo dalších důležitých komodit mohou nastat, ale pouze ztráty na životech, zranění civilistů nebo škoda na civilním majetku jsou z hlediska proporcionality relevantními faktory.[494]

V otázce, co vlastně zakládá excesivní disproporcionalitu, se názory liší. Mezinárodní trestní tribunál pro bývalou Jugoslávii k této otázce uvedl,

488 Anti-access/Area-denial.

489 DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict & Security Law*. 2012, roč. 17, č. 2, s. 267.

490 Čímž pravidlo přímo zavazuje všechny jednotky řetězu, kterému jinak rozkaz k provedení vojenské operace směřuje.

491 Článek 51, odst. 5, písm. b) Dodatkového protokolu I, dále pak článek 57, odst. 2, písm. a) a článek 57, odst. 2, písm. b) tamtéž.

492 Viz ZIMMERMANN, Andreas. The Second Lebanon War: Jus ad bellum, jus in bello and the Issue of Proportionality. *Max Planck Yearbook of United Nations Law*, 2007, sv. 11, s. 99-141.

493 Viz Jensen 2003 op. cit.

494 Viz Dinstein 2012 op. cit., s. 270.

že *„při určení, jestli byl útok proporcionální, je nutné posoudit, jestli mohla rozumně dobře informovaná osoba v daných podmínkách a za rozumného použití dostupných informací očekávat excesivní civilní ztráty jako následek útoku."* [495]

Nedostatek jasných pravidel tak mění toto posuzování v očích některých spíše v umění, než vědu.[496] Problematickým aspektem v rámci posuzování proporcionality je i rozdílná povaha některých vojenských operací, resp. dosažitelných vojenských výhod. Vedlejší škodu je možné měřit objektivně, např. údajem o počtu mrtvých a zraněných nebo výší škody na majetku, kvantifikace vojenské výhody však může být problematická. Může směřovat k dosažení kvalitativního cíle, jako je např. vzdušná nadvláda,[497] což lze jen obtížně porovnávat s kvantifikovatelnými vedlejšími ztrátami.

Aplikace principu rozlišení, ochrany a proporcionality je v kyberprostoru ještě problematičtější, protože kyberprostoru primárně nenáleží některé běžné charakteristiky. Za prvé dochází, ve smyslu obecné části tohoto textu, k přirozené deformaci geografické blízkosti. Tím dále dochází k prohlubování změn souvisejících s výše zmíněným nasazením dělostřelectva a letectva v 1. světové válce. Následné nasazení strategických bombardérů velkého doletu a strategických mezikontinentálních střel vedlo k narušení konceptu vzdálenosti, který je v rámci kyberprostoru již v podstatě neudržitelný. Bojiště se s jeho přesunem do kyberprostoru přesunulo ještě blíže k civilní populaci. Civilní přítomnost v oblasti s probíhajícími vojenskými operacemi, byť se jedná o přítomnost virtuální, je nevyhnutelná.[498]

Rostoucí závislost na počítačových systémech je tak jednou z hlavních obav v souvislosti s kybernetickými operacemi. Značná část vojenských informačních procesů spoléhá na civilní infrastrukturu nebo zároveň poskytuje své kapacity civilnímu informačnímu provozu.[499] Jedním z nejviditelnějších

495 Mezinárodní trestní tribunál pro bývalou Jugoslávii. *Prosecutor v. Stanislav Galić, Judgement and Opinion of 5 December 2003*. Dostupné z: http://www.icty.org/x/cases/galic/tjug/en/gal-tj031205e.pdf. Odst. 58.
Je zde možné pozorovat přímou vazbu na čl. 51 odst. 5 písm. b) Dodatkového protokolu I.

496 Viz Dinstein 2012 op. cit., s. 271.

497 Tamtéž.

498 Viz Lin 2012 op. cit., s. 523.

499 Viz DROEGE, Cordula. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 2012, roč. 94, č. 886, s. 538.

příkladů tak je např. používání navigačního systému GPS civilními vozidly. GPS přitom představuje primárně vojenskou technologii a v rámci vojenských operací hraje zcela zásadní roli. Samozřejmě některé počítače nebo sítě mohou sloužit jako výhradně vojenské, např. jako součást zbraní nebo zbraňových systémů. I civilní systém se ale může stát legitimním cílem kybernetické operace ve chvíli, kdy je použit kombatantem[500] nebo obecně k vojenskému účelu. Tato vlastnost kyberprostoru podrývá jeden ze základních předpokladů mezinárodního práva humanitárního, tedy že objekty jsou ze značné části odlišitelné jako vojenské nebo civilní.[501]

Kybernetické operace mohou být cílené na čistě vojenské cíle, např. radarová pole nebo C⁴ISR schopnosti protivníka, bez rizika vedlejších škod, resp. s rizikem menším, než je tradiční operace provedená kinetickými prostředky.[502] Na druhé straně je ale poměrně obtížné předvídat konkrétní důsledky kybernetických operací ve chvíli, kdy je cílem systém připojený do sítě a prostředkem napadení je škodlivý kód. Sekundární efekt operace nemusí být limitován striktně na vojenský cíl,[503] ale může dojít k řetězovému selhání.[504] Možnost řetězového selhání je vždy přítomná a k náležitému posouzení rizika je třeba úroveň znalostí nepřátelských systémů a jejich propojení, která často přesahuje znalosti odpovědných osob a informace jim dostupné. Sekundární efekt operace tak nemusí být limitován striktně na vojenský cíl. Tyto projevy komplexity provázaných systémů komplikují rozumnou aplikaci principu rozlišování. Domníváme se, že tyto schopnosti a vlastnosti by měly být v budoucnu rozumně očekávány ve chvíli, kdy dochází k vedení operací v kyberprostoru. Nepřizpůsobení operačních a organizačních paradigmat nemůže být omluvou pro nedůslednou aplikaci existujících pravidel.[505]

Ze shora uvedených vlastností kyberprostoru tak vyplývají dvě otázky, kdy jedna se vztahuje k cílení systému a k otázce excesivní disproporcionality operace vůči němu vedené vzhledem k vedlejším civilním škodám. Druhou je otázka, nakolik je civilní IT odborník způsobilý stát se vojenským cílem.

500 Srov. Dinstein 2012 op. cit., s. 263.
501 Viz Droege 2012 op. cit., s. 541.
502 O'DONNELL, Brian T. a James KRASKA. Humanitarian law: Developing International Rules for the Digital Battlefield. *Journal of Conflict & Security Law,* 2003, roč. 8, č. 1, s. 158.
503 Srov. Droege 2012 op. cit., s. 538.
504 Viz Jensen 2003 op. cit., s. 1178-79.
505 Viz Lin 2012 op. cit., s. 523.

V rámci odpovědi na první otázku je nutné definovat vojenský cíl. Poprvé se tento pojem objevil ve čl. 24 odst. 1 Pravidel leteckého boje jako *„objekt, jehož destrukce nebo zranění představuje konkrétní vojenskou výhodu pro strany konfliktu."*[506]

V současné době je pojem zakotven ve čl. 52 odst. 1 Dodatkového protokolu I, který byl již zmíněn, jako objekt, z jehož povahy, lokality, účelu nebo použití vyplývá efektivní přispění k nepřátelskému vojenskému snažení a jehož celkové nebo částečně zničení, obsazení nebo vyřazení z provozu vede k získání specifické vojenské výhody. Za objekt je tak považováno něco viditelného a hmotného[507] a z výkladu existujících pravidel se nejedná o data *per se*.[508] V případě operace vedené proti procesům kritické infrastruktury necílíme procesy, ale skrze procesy právě onen viditelný a hmotný objekt. Objekt se může stát cílem ve chvíli, kdy je přímo užíván ozbrojenými silami.[509] Zbraňové systémy nebo již zmíněné C^{4}ISR kapacity představují logický a nezpochybnitelně legální cíl. Civilní povaha personálu obsluhujícího tyto systémy je z hlediska možnosti systému stát se legálním cílem kybernetické operace irelevantní.[510] V případě kinetického útoku by tento aspekt irelevantní nebyl a muselo by být vyhodnoceno, zdali je útok proporcionální ke způsobeným civilním ztrátám.

Objekt se může stát vojenským cílem svojí polohou, pokud v dané oblasti přispívá vojenským snahám protivníka[511] a kybernetická operace tak může být provedena za účelem odepření efektivního využití geograficky určeného místa protivníkem. Objekt se může stát vojenským cílem svým použitím za vojenským účelem bez ohledu na původně civilní povahu. Pokud tedy ozbrojené složky převezmou kontrolu nad civilní sítí, okamžitě se stává vojenským cílem podle tohoto kritéria.[512] Pokud je použití systému ozbrojenými

506 Překlad autor. *The Hague Rules of Air Warfare, December 1922-February 1923*. Dostupné z: http://lawofwar.org/hague_rules_of_air_warfare.htm
Preambule, překlad autor. *Laws of War: Laws and Customs of War on Land (Hague II); July 29, 1899*. Dostupné z: http://avalon.law.yale.edu/19th_century/hague02.asp.

507 Sandoz 1987 op. cit., odst. 2007-2008.

508 Viz Tallinn Manual op. cit., s. 136 (pravidlo 39, odst. 5). K diskuzi MAČÁK, Kubo. Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law. *Israel Law Review*, 2015, roč. 48, č. 1, s. 55-80.

509 Sandoz 1987 op. cit., odst. 2020.

510 Tallinn manual op. cit., s. 126 (pravidlo 38, odst. 6).

511 Tamtéž, s. 127 (pravidlo 38, odst. 7).

512 Sandoz 1987 op. cit., odst. 2022.

složkami ukončeno, objekt přestává být vojenským cílem.[513] Objekt se může stát vojenským cílem svým účelem ve chvíli, kdy je určen pro budoucí vojenské užití.[514] Opatření spolehlivých zpravodajských informací je v tuto chvíli pro správné určení účelu objektu naprosto esenciální.[515]

Pro zachování funkce principu rozlišení je tedy, na základě výše uvedených ukazatelů, nutné rozhodnout, zdali je objekt vojenským cílem či nikoli. Pokud spadá pod rozsah jednoho z výše uvedených kritérií, může se legálně stát cílem kybernetické operace.

Na základě norem obsažených v mezinárodních smlouvách i identifikovaných jako součást práva zvykového je možné říci, že koexistence civilního objektu a vojenského cíle je nemožná. Ve chvíli, kdy je systém používán pro civilní i vojenské účely, převažuje vojenské použití systému a efektivně zbavuje daný systém absolutní ochrany vyhrazené civilním objektům. Jeho částečně civilní povaha se projevuje v nutnosti zabývat se proporcionalitou útoku a dá se tedy vnímat jako materiální korektiv. Žádná kybernetická operace cílící na zmíněný systém nesmí způsobit škodu, které by byla neproporcionální ve vztahu k získané vojenské výhodě.[516] Znovu tak musíme zdůraznit zcela zásadní aspekt získávání spolehlivých zpravodajských informací o cíli a o jeho provázanosti s ostatními systémy. Jestli je míra vojenského použití systému důležitá pro posouzení proporcionality vojenské operace vedené vůči němu zůstává nevyřešenou otázkou.

Při rozhodování se mezi kinetickým útokem a kybernetickou operací může být kybernetická operace výrazně upřednostňována. Pokud nahlédneme do praxe věnující se leteckému bombardování, můžeme najít i názory uvádějící, že obecně lze velkou elektrárnu postavenou tak, aby poskytovala energii strategickému přístavu a námořní základně považovat za objekt, jehož destrukce představuje konkrétní vojenskou výhodu,[517] která je dostatečně specifická a přímá k tomu, aby operaci legalizovala. Proporcionální posouzení, umožňující nám dospět k preferenčnímu použití kybernetické

513 Tallinn manual op. cit., s. 129 (pravidlo 38, odst. 10)
514 Sandoz 1987 op. cit., odst. 2022.
515 Tallinn manual op. cit., s. 129 (pravidlo 38, odst. 11-12.)
516 Tamtéž, s. 126 (pravidlo 38, odst. 2-3.).
517 Eritrea-Ethiopia Claims Commission – Partial Award: Western Front, Aerial Bombardment and Related Claims – Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 & 26. United Nations, 2009. Dostupné z: http://legal.un.org/riaa/cases/vol_XXVI/291-349.pdf. Odst. 121.

operace můžeme naplnit s poukazem na dikci čl. 57 Dodatkového protokolu I. Ten stanovuje, že v případě možné volby mezi několika cíli umožňujícími dosažení stejné vojenské výhody má být cíl stanoven tak, aby útokem došlo k co možná nejmenšímu nebezpečí pro civilní životy a objekty. Útok na vojenský cíl prostřednictvím kybernetické operace může být proporcionálnější, než je použití kinetických prostředků ke zničení daného cíle. Dočasné vyřazení SCADA/CPS systémů cílí kritickou infrastrukturu primárně jako proces a nekinetické vyřazení z provozu tak může být proporcionálnější v porovnání s vyřazením z provozu kinetickými prostředky.

Na druhou stranu je nutné si uvědomit, že absolutní upřednostňování kybernetických operací může některé výhody proměnit v nevýhody. Pokud k problematice přistoupíme zcela pragmaticky, civilní oběti mohou vytvářet tlak mezi vlastní populací útočícího státu,[518] který směřuje k ukončení vojenských operací a hledání smírného řešení. Odstranění „počítání mrtvých" ve formě vedlejších škod může odstranit tento příslovečný Damoklův meč visící nad politickou reprezentací. Kelsey také uvádí, že bojující strany mohou být ochotnější cílit i na civilní systémy nebo systémy se zanedbatelnou povahou vojenského užití ve chvíli, kdy jsou užité prostředky primárně nekinetické.[519] Může sice dojít k sekundárně kinetickému následku operace a kauzálním ztrátám na životech nebo škodách na majetku. I v tu chvíli však existuje značná míra popiratelnosti kauzálního propojení operace a způsobených škod. Vyjasnit vztah mezi primárně nekinetickou a sekundárně kinetickou povahou kybernetické operace je tak nutné i z hlediska jasného výkladu a aplikace existujícího právního rámce.

V otázce přímé účasti hackerů nebo IT expertů na kybernetických operacích se stal v textu již několikrát zmiňovaný Tallinnský manuál v kruzích veřejnosti textech značně odsuzovaným. Zprávy často uváděly, že manuál poskytuje ospravedlnění pro zabíjení hackerů či hacktivistů. Hlavním problémem byly aktivity tzv. hnutí Anonymous a otázka, zda je jejich aktivity[520]

518 V duchu okřídleného novinářského „if it bleeds, it leads".

519 KELSEY, Jeffrey. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*, 2008, roč. 106, č. 7, s. 1436, 1439-1441.

520 Manuál explicitně nezmiňuje Anonymous, ale je očividně, že byla tato část psána s důrazem právě na jejich činnost.

mohou učinit legálním cílem pro likvidaci prostřednictvím dronů. Tallinnský manuál přitom vychází z explicitně formulované premisy, že veškeré kybernetické operace, které se odehrávají v rámci ozbrojeného konfliktu, podléhají pravidlům humanitárního práva.[521] Toto zcela jasné, přesto opomíjené, vymezení má pro další diskuzi o případném cílení hackerů zásadní význam. Cílení hackerů nebo IT expertů je totiž v rámci konfliktu automaticky limitováno požadavky na rozlišení, ochranu a proporcionalitu. Anonymous jako skupina nemají v současné době prostředky a potenciál naplnit podmínky stanovené soudem v rámci rozhodnutí Tadić.[522] Jejich činnost spočívá primárně v DDoS útocích, mazání dat, defacementu webových stránek, „krádeži" dat a podobných aktivitách. Žádná z těchto aktivit není sama o sobě schopna být užitím síly, takže ani doktrína akumulace událostí nezpůsobí, aby byla aktivita Anonymous vnímána optikou ozbrojeného konfliktu.[523]

Co se týká civilních IT expertů účastnících se konfliktu, zde je situace odlišná. Důležitou otázkou je, jaká konkrétní činnost zakládá přímou účast na konfliktu. Jak totiž bylo zmíněno, civilisté jsou chráněni pouze do chvíle, než se konfliktu přímo zúčastní.[524] V takovém případě ochranu plynoucí z jejich civilního charakteru po dobu své přímé účasti ztrácí.[525] Aby mohlo být jednání chápáno jako přímá účast na konfliktu, musí tato činnost negativně ovlivňovat vojenské operace nepřítele a musí existovat identifikovatelný kauzální nexus mezi jednáním a negativním efektem na probíhající operaci. Jednání také musí být v přímém vztahu k nepřátelské operaci.[526] Jakmile dojde ke kumulativnímu splnění všech těchto kritérií, přestává být civilní specialista předmětem ochrany. Kybernetické operace i operace mimo kyberprostor mířící k vyřazení této osoby z aktivní činnosti jsou pak legální.

521 Tallinn manual op. cit., s. 75 (pravidlo 20).

522 Mezinárodní trestní tribunál pro bývalou Jugoslávii. *Prosecutor v. Tadić – Opinion and Judgment of 7 May 1997*. Dostupné z: http://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf

523 Tallinn manual op. cit., s, 87-88 (pravidlo 23, odst. 8).

524 Článek 51, odst. 3 Dodatkového protokolu I a článek 13 odst. 3 Dodatkového protokolu II.

525 To klade zcela zásadní nároky na vojenské síly, které jsou cílem taktiky *udeř a uteč*. Civilisté, účastnící se těchto operací jsou cílem pouze od úderu do útěku – od útěku do dalšího úderu jsou chráněni. Viz Schmitt 2010 op. cit., s. 834.

526 MELZER, Nils. *Interpretative Guidance on the Notion of Direct Participation on Hostilities Under International Humanitarian Law*. Geneva: ICRC, 2009. Dostupné z: https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf. S. 47, 51 a 58.

Existuje několik možností, jak se může civilní IT expert zapojit do ozbrojeného konfliktu. Provedení ofenzivní kybernetické operace přímo navázané na ozbrojený konflikt konstituuje přímou účast bez ohledu na civilní povahu odborníka. Naopak udržování důvěrnosti, integrity a dostupnosti vlastní sítě nebo jednotlivého počítače není způsobilé konstituovat přímou účast na konfliktu, bez ohledu na povahu pozdějšího použití dané sítě nebo přístroje.[527] Kybernetická operace směřující k vyřazení systému totiž aspiruje posílení kapacit vlastních a oslabení kapacit nepřátelských. Prevenční činnost ve vztahu k této operaci, která jí zabrání v úspěchu, nevede k oslabení nepřátelských vojenských schopností ani posílení schopností vlastních. Není tedy překročen práh negativního vlivu a první kritérium ze tří výše uvedených není naplněno. Účast na aktivních protiopatřeních naproti tomu může být vnímána jako aktivní účast na vedení boje – značně zde záleží na provedení konkrétního protiopatření, resp. na schopnosti protiopatření umenšit bojové schopnosti nepřítele. Jakmile se IT expert neomezuje na udržování důvěrnosti, integrity nebo dostupnosti vlastního systému, ale míří proti těmto hodnotám u systému nepřátelského, dochází zřejmě k jeho přímé účasti na konfliktu. Po dobu jeho účasti je tak legální ho zneškodnit a nedochází tím, přes jeho původně civilní povahu, k porušení norem mezinárodního humanitárního práva.

Shora uvedené ukazuje, kudy se v současném světě ubírají diskuze o aplikaci mezinárodního práva na problematiku kybernetické bezpečnosti (zahrnující i ofenzivní kybernetické operace). Rozhodně nelze konstatovat, že by mezinárodní právo nedopadalo na tyto operace. Kyberprostor a jednání v něm nepředstavuje v těchto intencích právní vakuum. Na druhé straně má mezinárodní právo jen velmi malou dynamiku. Využití Martensovy klauzule pro posun výkladu je spíše diskusního charakteru, byť má své místo. Jsou to zejména státy, které vytváří mezinárodní právo – v poslední době nicméně jako by vyklízely pozice[528] ve prospěch normotvorby[529] ze strany nestátních a mezinárodních organizací.[530] Jedná se velmi důležité téma pro národní

527 Tallinn manual op. cit., s. 120 (pravidlo 35, odst. 5)

528 Vzácnou výjimkou je např. *opinio juris* vyjádřené v Koh 2012 op. cit.

529 Srov. Finnemore 1998 op. cit.

530 MAČÁK, Kubo. Is International Law of Cyber Security in Crisis? In: PISSANIDIS, Nikolaos, ROIGAS, Henry a Matthijs A. VEENENDAAL. *2016 8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2016. S. 134-136.

kybernetickou bezpečnost – otázky na legalitu konkrétních postupů se objevují opakovaně i v České republice. Lze tak jen doporučit aktivizaci orgánů a formulaci konkrétního postoje k některým shora uvedeným problémům. Těžko si představit, že by Česká republika diktovala tempo vývoje, ale zaujetí konkrétního postoje k některým právním otázkám pomůže zformulovat národní zájmy v kyberprostoru. Je vhodné si uvědomit, že současná situace je právně nejistou. Napravení tohoto stavu a formulování pozice, jak bude stát vnímat kybernetické operace proti němu vedené, je mimořádně žádoucí.

SUMMARY

The Czech Republic was the first EU member state that introduced a complex cybersecurity legislation covering public and private sector. The regulatory model of the Czech Cybersecurity Act is in principle analogous to the Network Information Security (NIS) Directive that was adopted a year and a half later.

The Czech cybersecurity legal regulatory framework, besides acting in many ways as a pioneering solution and a proof of concept, contains a number of innovative elements. First of all, it works, quite uniquely in the Czech context, with performance-based rules that set only fundamental regulatory standards and let the regulated subjects to choose their own particular normative solutions.

This regulatory model was chosen because it turned out that subjects covered by the new security obligations (namely those that operate critically important information systems or networks) are mostly actively willing to establish proper information security solutions and there was a good prospect that they will not categorically refuse or resist these new obligations. It was also assumed (rightly, as it turned out later) that the regulation can be mostly efficient not through one or more standard sets of particular legal requirements, but that it might work better if each security solution can be uniquely specific and tailored to respective information system or network. In that sense, it was obvious that there is nobody positioned better in order to determine which tools to use for mostly efficient securing of respective systems or networks than their owners or controllers.

Another specific feature of the Czech Cybersecurity legal regulatory framework is the implementation of two central response teams (CERTs) – the Governmental and the National. The Governmental CERT is the central Czech response team that is run by the national cyber-authority (currently the Nationaly Security Authority that will be later this year merged to National Cybersecurity and Information Security Authority) – it directly administers critically important information systems and networks and it is also designated as the central Czech cyber-bureau and contact point.

The National CERT is run by a private entity (currently by the national domain authority – the CZ.NIC) and its task is to provide for CERT capabilities mostly for the part of private sector that falls outside of the constituency of the Governmental CERT. The National CERT is subordinate to the Governmental CERT, but it is operated relatively independently

on a private-law basis which makes it a better partner for voluntary cooperation with various business and academic entities.

Third special feature of the Czech cybersecurity regulatory architecture is definitely to be found in some of its fundamental principles. The whole regulation is, quite surprisingly, not philosophically based on the protection of public or national security. The fundamental philosophical concept that serves as a teleological ground for all regulatory elements of the Czech cybersecurity statutory framework is rather the protection of the right of informational self-determination and other fundamental rights. It is assumed that individuals might exercise their individual information rights (privacy, freedom of information, freedom of speech etc.) only if the environment created by information society services is properly secured. Moreover, in a situation when many core societal functionalities are depending on functioning information network, it is of vital importance also for other fundamental rights (life, health, property etc.) to keep the information environment safe.

We have a good reason to believe that this approach positioning fundamental rights to the very core of the overall teleology of the Czech Cybersecurity Act (together with other standard principles such as technology neutrality) also helped the original Cybersecurity Bill to smoothly make its was through the legislative process. In that sense, it is to be especially noted that the whole legislative procedure did not take more than a year despite of extremely turbulent political development in that time - the Bill was originally put forward by a conservative government, then there came a government of technocrats when the Bill was pending in the House of Representatives and the whole procedure was finished by a socialist government – all that without changing almost anything from the first draft.

There are a number of other extraordinary, unusual or inspiring issues around the Czech cybersecurity legal regulatory framework not all of which are, of course, completely positive. This book tries to critically tackle most of them and to provide for a complex understanding of the Czech take on the legal regulatory phenomenon of cybersecurity in broadest possible context. In addition, the book also discusses problems and questions that are not currently tackled in Czech legal practice but that, as we believe, will soon emerge – such as public international law liability of states for non-acting against cybersecurity incidents, individual liability or professionals or amateur users for security faults, development of cyber diplomacy and international agenda in cyber-development etc.

LITERATURA A DALŠÍ POUŽITÉ ZDROJE

ALEXY, R. On the Structure of Legal Principles. Ratio Iuris. 2000, roč. 13, č. 3.

ALEXY, R. The Argument from Injustice, přel. Paulson, S., Litschewski Paulson, B. Oxford: Oxford University Press, 2002.

ANNAN, Kofi. Two Concepts of Sovereignty. *The* Economics, 1999, 16th September. Dostupné z: http://www.economist.com/node/324795.

APPLEGATE, Scott. The Dawn of Kinetic Cyber. In: PODINS, Karlis; STINISSEN, Jan; MAYBAUM, Markus. *2013 5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2013.

AUJEZDSKÝ, J. Skutečně může zaměstnavatel číst Vaší poštu?, server it-pravo.cz, 20. 1. 2004.

BALBANIAN, N. Presumed Neutrality of Technology, Society, roč. 17, číslo 3.

BAMBAUER, D. Privacy versus Security, The Journal of Criminal Law & Criminology, roč. 103, číslo 3.

BANDE, L. C. A Case for Cybercrime Legislation in Malawi, Malawi Law Journal, roč. 5.

BARKHAM, Jason. Information Warfare and International Law on the Use of Force. *New York University Journal of International Law & Politics*, 2001, roč. 34, č. 1.

BARNES, Darryl T. Content Monitoring Issues Legal and Otherwise. SANS Institute. 2009.

BAROŠ, J. (ed.) Vladimír Čermák – člověk, filozof, soudce. Brno: Masarykova univerzita, 2009.

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

BENIGER, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA, USA: Harvard University Press, 1986.

BENKLER, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press, 2006.

BEREJKA, M. A Case for Government Promoted Multi-Stakeholderism, Journal on Telecommunications and High-Tech Law, roč. 10, str. 9.

BERNSTEIN, A. What We Talk About When We Talk About Workplace Privacy, Louisiana Law Review, roč. 66, číslo 4, str. 923, ke stažení on-line na adrese http://digitalcommons.law.lsu.edu/lalrev/vol66/iss4/2.

BĚLINA, M. a kol. Pracovní právo. 5. dopl. a podstat. přeprac. vyd., Praha: C. H. Beck, 2012.

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

BRENNER, S. Cyber-threats and the Limits of Bureaucratic Control, Minnesota Journal of Law, Science and Technology, roč. 14, číslo 1.

BUCHAN, Russell. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict & Security Law*, 2012, roč. 17, č. 211-227.

CASSESE, Antonio. The Martens Clause. Half a Loaf or Simply Pie in the Sky? *European Journal of International* Law, 2000, roč. 11, č. 1.

CECIL, Alisha. *A summary of network traffic monitoring and analysis techniques*. Computer Systems Analysis, 2006, 4-7.

CLARKE, Richard A. a Robert KNAKE. *Cyber War*, 2010.

CORMACK, A. Can CSIRTs Lawfully Scan for Vulnerabilities? *SCRIPTed*, roč. 11, č. 3.

DE CARVALHO, Benjamin, HALVARD, Leira a John M. HOBSON. The Big Bangs of IR: The Myths That Your Teachers Still Tell You about 1648 and 1919. *Millenium*, 2011, roč. 39, č. 3.

DE JOUVENEL, Bertrand. *Sovereignty: An Inquiry Into the Political Good*. Chicago: University of Chicago Press, 1957.

DEJEAN, S., PÉNARD, T., SUIRE, R. Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, Rennes: CREM, ke stažení on-line na adrese http://www.01net.com/genere/article/fichiersAttaches/300415066.pdf.

DEVOST, M. G., MOSS, J. POLLARD, N. A. STRATTON, R. J. III. All Done Except the Coding, Georgetown Journal of International Affairs, roč. 11.

DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict & Security Law*. 2012, roč. 17. č. 2.

DONALDSON, Scott E., Stanley G. SIEGEL, Chris K. WILLIAMS a Abdul ASLAM. Cybersecurity Frameworks. Enterprise Cybersecurity [online]. Berkeley, CA: Apress, 2015, s. 297 [cit. 2016-11-03]. DOI: 10.1007/978-1-4302-6083-7_17. ISBN 978-1-4302-6082-0. Dostupné z: http://link.springer.com/10.1007/978-1-4302-6083-7_17.

DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. *Řízení bezpečnosti informací*. 2. vydání. Praha: Professional publishing, 2011, 240 str., ISBN 978-80-7431-050-8.

DROEGE, Cordula. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 2012, roč. 94, č. 886.

DWORKIN, R. Justice for Hedgehogs, London: Belknap Press, 2011.

DWORKIN, R. Justice in Robes. London: Belknap Press, 2006.

DYZENHAUS, David. *Legality in a Time of Emergency*. Cambridge: Cambdridge University Press, 2006.

ESSER, J. Vorverständnis und Methodenwahl in der Rechtsfindung: Rationalitatsgrundlagen richterlicher Entscheidungspraxis, Frankfurt: S. Fisher, 1972.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. 2015. ISBN 978-92-9204-131-1.

EVANS, Tyler D. At War with the Robots: Autonomous Weapon Systems and the Martens Clause. *Hofstra Law Review*, 2013, roč. 41, č. 3.

FEDER, Norman Menachem. Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack. *New York University Journal of International Law and Politics*, 1987, roč. 19, č. 2.

FINNEMORE, Martha a Kathryn SIKKINK. International Norm Dynamics and Political Change. *International Organization*, 1998, roč. 52, č. 4.

FINNIS, J. Natural Law. New York: New York University Press, 1991.

FLECK, Dieter. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict & Security Law*. 2013, roč. 18, č. 2.

FLECK, Dieter (ed.). *The Handbook of Humanitarian Law in Armed Conflicts*. Oxford University Press: Oxford/New York, 1995.

FREDLAND, J. S. Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies, Military Law Review, číslo 206.

FREILING, F. C., HORNUNG. G. POLČÁK, R. (eds.); Forensic Computing – report from Dagstuhl Seminar 13482, Dagstuhl, Dagstuhl Publishing, 2014.

GALVAS, M. a kol. Pracovní právo. Brno: Masarykova univerzita, 2012.

GARTZKE, Erik. The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, 2013, roč. 38, č. 2.

GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: CCD COE Publications, 2011.

GEERS, Kenneth, THOMPSON, Kevin a Abhishek PIDWA. *Leviathan? Command and Control Communications on Planer Earth*. Black Hat Las Vegas, 2014. Dostupné z: https://www.blackhat.com/docs/us-14/materials/us-14-Geers-Leviathan-Command-And-Control-Communications--On-Planet-Earth-WP.pdf.

GELLER, Eric. Your complete guide to the 5 cybersecurity bills in Congress. The Daily Dot [online]. 2015 [cit. 2016-01-2]. Dostupné z: http://www.dailydot.com/politics/congress-cybersecurity-threat-sharing-bills-explained-cisa-cispa-pcna/.

GLENNON, M. The Dark Future of International Cybersecurity Regulation, Journal of National Security Law and Policy, roč. 6.

GONG, Wenxiang. Information Sovereignty Reviewed. *Intercultural Communication Studies*, 2005, roč. 14, č. 1, s. 119-135.

GORDON, Lawrence A.; LOEB, Martin P.; LUCYSHYN, William. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 2003, 22.6: 461-485.

GRAHAM, James; HOWARD, Richard; OLSON, Ryan (eds.). *Cyber Security Essentials*. Boca Raton: CRC Press, 2011.

GRANT, J. Will There Be Cybersecurity Legislation? Journal of National Security Law and Policy, roč. 4.

GROUP, Tom. Why Cybersecurity Information Sharing Is Important. RSA Conference [online]. 2016 [cit. 2016-11-06]. Dostupné z: https://www.rsaconference.com/blogs/why-cybersecurity-information-sharing-is-important.

HABER, Eldar. The French Revolution 2.0: Copyright and the Three Strikes Policy. *Harvard Journal of Sports and Entertainment Law*, 2011, roč. 2, č. 2.

HANSEN, Lene a Helen NISSENBAUM. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 2009, roč. 53, č. 4.

HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. Revue pro právo a technologie. 2015, 6(12), 22. ISSN 1805-2797.

HATHAWAY, M. E., KLIMBURG, K. Preliminary Considerations: On National Cybersecurity, in Klimburg, A. National Cybersecurity – Framework Manual, Talinn: CCDCOE, 2012.

HATHAWAY, Oona A., CROOTOF, Rebecca, LEVITZ, Philip a Haley NIX. Law of Cyber-Attack. C*alifornia* Law Review*,* 2012, roč. 100, č. 4.

HESSBRUEGGE, J. A. The Historical Development of the Doctrines of Attribution and Due Dilligence in International Law.

HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007. Dostupné z: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

HOLLÄNDER, P. Filosofie práva. Plzeň: Aleš Čeněk, 2006.

HOLLÄNDER, P. Materiální ohnisko ústavy a diskrece ústavodárce, Právník, roč. 2005, č. 4.

HOLLÄNDER, Pavel. *Základy všeobecné státovědy*. 3. vydání. Plzeň: Aleš Čeněk, 2012.

HUME, D. A Treatise on Human Nature. Project Gutenberg, 2003, dostupný on-line na adrese www.gutenberg.org/etext/4705.

HUSOVEC, M. Zodpovednosť na internete podľa českého a slovenského práva, Praha: CZ.NIC, 2014, ke stažení on-line na adrese http://knihy.nic.cz/files/nic/edice/Zodpovednost_web_FINAL.pdf.

HYLTON, K. N.: Property Rules, Liability Rules, and Immunity: An Application to Cyberspace, Boston University Law Review, roč. 87, číslo 1.

JAMES, Alan. The Practice of Sovereign Statehood in Contemporary International Society. *Political* Studies, 1999, roč. 47, č. 3, s. 457-473.

JAMES, W. Pragmatism. Rockville: ARC Manor, 2008.

JAMNEJAD, Maziar a Michael WOOD. The Principle of Non-intervention. *Leiden Journal of International Law*, 2009, roč. 22, č. 2.

JENSEN, Eric Talbot. Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? *American University International Law Review*, 2003, roč. 18, č. 5.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

JOYNER, Christopher C. a Catherine LOTRIONTE. Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, 2001, roč. 12, č. 5.

KELLY, T. K., HUNKER, J. Cyber Policy: Institutional Struggle in a Transformed World, I/S: Journal of Law and Policy, roč. 8, číslo 2.

KELSEN, H. Pure Theory of Law, přel. Knight, M. Berkeley: University of California Press, 1978.

KELSEY, Jeffrey. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*, 2008, roč. 106, č. 7.

KESAN, J. P.; HAYES, C. M.: Creating a 'Circle of Trust' to Further Digital Privacy and Cybersecurity Goals, Illinois Public Law Research Paper No. 13-03, vyjde v Michigan State Law Review.

KESAN, J. P., HAYES, C. M. Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace, Harvard Journal of Law and Technology, roč. 25, číslo 2.

KNAPP, V. Některé úvahy o odpovědnosti v občanském právu. Stát a právo I. roč. 1956.

KODAR, Erki. Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I. In: LIIVOJA, Rain a Andres SAUMETS (eds.). *The Law of Armed Conflict: Historical and Contemporary Perspectives*. Tartu University Press: Tartu, 2012.

KOH, Harold Hongju, International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Ganecy Legal Conference Fr. Meade, MD, Sept. 18, 2012. *Harvard International Law Journal Online*, 2012, roč. 54, dostupné na http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

KOOPS, Bert-Jaap, NEWELL, Bryce Clayton, TIMAN, Tjerk, ŠKORVÁNEK, Ivan, CHOKREVSKI, Tom a Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law* [přijato k publikaci]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043.

KOŠIČIAROVÁ, S. Princípy dobrej verejnej správy a Rada Európy, Bratislava: Iura Edition, 2012.

KRETZMER, David. The Inherent Right to Self-Defence and Proportionality in Jus ad Bellum. *The European Journal of International Law*, 2009, roč. 20, č. 2.

KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Vyd. 1. Praha: C. H. Beck, 2012. 516 s. Beckova edice komentované zákony. ISBN 9788071792260.

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

LAUTERPACHT, Eli. Sovereignty-Myth or Reality. *International Affairs*, 1997, roč. 73, č. 1.

LAVICKÝ, P. a kol.: *Občanský zákoník I.* Obecná část (§ 1−654). Komentář. 1. vydání, Praha: C. H. Beck, 2014.

LEE, Ronald M & Thomas RID. OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy. *The RUSI Journal*, 2014, roč. 159, č. 5.

LESSIG, L. Code V. 2. New York: Basic Books, 2006.

LEVIN, A. Is There a Global Approach to Workplace Privacy? in Zureik, E., Stalker, L. H., Smith, E., Lyon, D., Chan, Y. E. Surveillance, Privacy and the Globalization of Personal Information, Montreal: cGill-Queen's University Press, 2010.

LIBICKI, Martin C. Sharing Information About Threats Is Not a Cybersecurity Panacea. Technical report, RAND, 2015.

LIN, Herbert. Cyber conflict and international humanitarian law. *International Review of the Red Cross,* 2012, roč. 94, č. 886.

LIN, H. Thoughts on Threat Assessment in Cyberspace, Journal of Law and Policy for the Information Society, roč. 8, číslo 2.

LIVINGSTONE, David a Patricia LEWIS. *Space, the Final Frontier for Cybersecurity?* Chatham House, 2016. Dostupné z: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity.

MACCORMICK, Neil. Beyond the Sovereign State. *Modern Law Review*, 1993, roč. 56, č. 1.

MAČÁK, Kubo. Is International Law of Cyber Security in Crisis? In: PISSANIDIS, Nikolaos, ROIGAS, Henry a Matthijs A. VEENENDAAL. *2016 8th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2016.

MAČÁK, Kubo. Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law. *Israel Law Review*, 2015, roč. 48, č. 1.

MATEJKA, J. Internet jako objekt práva – hledání rovnováhy autonomie a soukromí, Praha: CZ.NIC, 2013, k dispozici též on-line ke stažení na adrese https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

MATES, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, 2006.

MCDOUGAL, Myres. Law as a Process of Decision: A Policy-Oriented Approach to Legal Study. *Natural Law Forum*, sv. 1.

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

MELZER, Nils. *Interpretative Guidance on the Notion of Direct Participation on Hostilities Under International Humanitarian Law*. Geneva: ICRC, 2009. Dostupné z: https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf.

MERON, Theodor. The Martens Clause, Principles of Humanity, and Dictates of Public Conscience. *The American Journal of International Law*, 2000, roč. 94, č. 1.

MINAŘÍK, Pavel. *Pokročilá analýza provozu datových sítí*. IT Systems [online]. 2015, 2015(1) [cit. 2016-07-08]. Dostupné z: https://www.systemonline.cz/it-security/pokrocila-analyza-provozu-datovych-siti.htm.

MORGENTHAU, Hans Joachim. *Politics among nations: the struggle for power and peace.* Boston: McGraw-Hill, 1993.

MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů*. Brno: Masarykova univerzita, 2013.

NOEIM, G. T. Cybersecurity and Freedom on the Internet, Journal of National Security Law & Policy, roč. 4.

NOEIM, G. T.: Cybersecurity: Ideas Whose Time Has Not Come-and Shouldn't, I/S: A Journal for Law and Policy, roč. 8, číslo 2.

NYE, Joseph. *The Future of Power*. New York: Public Affairs, 2011.

O'DONNELL, Brian T. a James KRASKA. Humanitarian law: Developing International Rules for the Digital Battlefield. *Journal of Conflict & Security Law,* 2003, roč. 8, č. 1.

OLIVEIRA, D. Cyber-Terrorism & Critical energy Infrastructure Vulnerability to Cyber-Attacks, Environmental & Energy Law & Policy Journal, roč. 5, číslo 2.

ONDRÁK, V., SEDLÁK, P., MAZÁLEK, V. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

OPPENHEIM, Adolf Leo. *International Law: A Treatise*. New York and Bombay: Longmans, Green, and Co., 1905. S. 117 (marg. č. 79). Dostupné z: https://archive.org/details/internationallaw12oppe.

PHILPOTT, Daniel. Sovereignty. *Stanford Encyclopedia of Philosophy*, publikováno 2003, upraveno 2016. Dostupné z: http://plato.stanford.edu/entries/sovereignty/.

POKORNÝ, L. Zpravodajské služby, Praha: Auditorium, 2012.

POLČÁK, R. Internet a proměny práva, Praha: AUDITORIUM, 2012.

POLČÁK, R. Internet Legal Culture, Lex Informatica and (un)Desired Sovereignty of Lawyers. In Lindskoug, P., Manusbach, U. Millqvist, G., Samuelsson, P., Vogel, H. H. Essays in Honour of Michael Bogdan. 1. vyd. Lund: Författarna och Juristförlaget i Lund, 2013.

POLČÁK, R. Nedovolené přesměrování při připojení k internetu v rozhodnutí Spolkového soudního dvora, Jurisprudence, roč. XIV, číslo 3

POLČÁK, R. Vygum v kyberprostoru: Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z. Information Security Summit 2011. 1. vyd. Praha: Data Security Management, 2011.

POLČÁK, R. Kybernetická bezpečnost jako aktuální fenomén českého práva, Revue pro právo a technologie, roč. 6, číslo 11, str. 95.

POLČÁK, R., ŘÍHA, Z., MALINKA, K. Právní aspekty interních směrnic - část I. Data Security Management, roč. XIX, číslo 2.

POLČÁK, R., ŘÍHA, Z., MALINKA, K. Právní aspekty interních instrukcí – část II. Data Security Management, roč. XIX., číslo 3.

PORSCHE, Isaac R. III, SOLLINGER, Jerry M., MCKAY, Shawn. *A Cyberworm that knows no Boundaries*. Santa Monica: RAND Corporation, 2011. Dostupné z: www.rand.org/pubs/occasional_papers/OP342.html.

POTOČNÝ, Miroslav. Otázka legality hrozby nebo použití jaderných zbraní. *Mezinárodní vztahy*, 1999, roč. 34, č. 1.

PUSTOGAROV, Vladimir Vasilievich. F*yodor Fyodorovich Martens (1845-1909) – a humanist of modern times*. Dostupné z: https://www.icrc.org/eng/resources/documents/article/other/57jn52.htm.

POWELL, B. Is Cybersecurity a Public Good? Evidence From the Financial Services Industry, Journal of Law, Economics and Policy, roč. 1, číslo 2.

RADBUCH, G. Gesetzliches Unrecht und übergesetzliches Recht, Süddeutsche Juristenzeitung, roč. 1946.

RORTY R. The Banality of Pragmatism and the Poetry of Justice. Southern California Law Review. 1990, roč. 63.

ROSCINI, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014.

ROSENZWEIG, P. Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?, Journal of Law and Policy for the Information Society, roč. 8, číslo 2.

ROWLAND, Jill, RICE, Mason a Sujeet SHENOI. Whither cyberpower? *International Journal of Critical Infrastructure Protection*, 2014, roč. 7, č. 2.

RUSTAD, M. L., PAULSSON, S. R. Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe, University of Pennsylvania Journal of Labor and Employment Law, roč. 7.

SALES, S. A. Regulating Cyber-Security, Northwestern University Law Review, roč. 107, číslo 4.

SALTER, Michael. Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 3.

SANDOZ, Yves, SWINARSKI, Christophe a Bruno ZIMMERMANN (eds.). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: International Committee of the Red Cross, 1987. Dostupné z: http://www.loc.gov/rr/frd/Military_Law/RC_commentary-1977.html.

SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 1999, roč. 37, č. 3.

SCHMITT, Michael. Military Necessity and Humanity. *Virginia Journal of International Law*, 2010, roč. 50, č. 4.

SCHMITT, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

SCHMITT, Michael N. The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski. In: CZOSSECK, Christian; Ottis, Rain; ZIOLKOWSKI, Katharina (eds.). *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, s. 311-317. ISBN 9789949904099.

SELMI, M. Privacy for the Working Class: Public Work and Private Lives, Louisiana Law Review, roč. 66, číslo 4.

SHANE, P. M. Cybersecurity Policy as if „OrdinaryCitizens" Mattered: The Case for Public Participation in Cyber Policy Making, Journal of Law and Policy for the Information Society, roč. 8, číslo 2.

SHARP, W.G. Sr. The Past, Present and Future of Cybersecurity, Journal of National Security Law and Policy, roč. 4, číslo 13.

ŠIMÍČEK, V. (ed.) Právo na soukromí. Brno: Mezinárodní politologický ústav, 2011.

ŠÍN Z.: Tvorba práva. Praha: C. H. Beck, 2003.

STONE, John. Cyber War Will Take Place. *Journal of Strategic Studies*, 2013, roč. 36, č. 1.

TAMANHA, B. Beyond the Formalist – Realist Divide. Princeton: Princeton University Press, 2010.

TAMS, Christian. The use of Force against Terrorists. *The European Journal of International Law*, 2009, roč. 20, č. 2.

TAYLOR, L. M. D. The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era, Minnesota Journal of Law, Science & Technology, roč. 15, číslo 2.

TIKK, Eneken. *Comprehensive Legal Approach to Cyber Security*. Tallinn, 2011. Disertační práce, University of Tartu, Právnická fakulta. Dostupné z: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1.

TOFFLER, Alvin a Heidi TOFFLER. *War and antiwar*. New York: Warner Books, 1993.

TOWNSHEND, Charles (ed.). The Oxford History of Modern War. Oxford: Oxford University Press, 2000.

TUBBS, David, LUZWICK, Perry a Walter Gary SHARP. Technology and Law: The Evolution of Digital Warfare. *International Law Studies*, 2002.

VOROBIEV, V. I., FEDORCHENKO, L. N., ZABOLOTSKY, V. P., LYUBIMOV, A. V. Ontology-based analysis of information security standards and capabilities for their harmonization, in Proceedings of the 3rd international conference on Security of information and networks, New York: ACM, 2010.

VYSOKAJOVÁ, M. Zákoník práce - komentář. Praha: Wolters Kluwer, 2012.

WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law*, 2011, roč. 36, č. 2.

WEILL, P., Woodham, R. Don't Just Lead, Govern: Implementing Effective IT Governance. MIT Sloan Working Paper No. 4237-02, 2002, dostupné on-line na adrese http://ssrn.com/abstract=317319.

WHEELWRIGHT, K. Monitoring Employees' Email and Internet Use at Work - Balancing the Interests of Employers and Employees, Journal of Law, Information and Science, roč. 13, číslo 1.

WONG, Derek. Sovereignty Sunk? The Position of 'Sinking States' at International Law. *Melbourne Journal of International Law*, 2013, roč. 14, č. 2.

YOO, C. S. Network Neutrality and the Economics of Congestion. Georgetown Law Journal, roč. 94.

ZAVRŠNIK, A.: Towards an Overregulated Cyberspace: A Criminal Law Perspective, Masaryk University Journal of Law and Technology, roč. 4, číslo 2.

ZIOLKOWSKI, Katharina. Ius ad bellum in Cyberspace – Some Thoughts on the „Schmitt-Criteria" for the Use of Force. In: CZOSSECK, Christian; Ottis, Rain; ZIOLKOWSKI, Katharina (eds.). *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.

ZIMMERMANN, Andreas. The Second Lebanon War: Jus ad bellum, jus in bello and the Issue of Proportionality. *Max Planck Yearbook of United Nations Law*, 2007, sv. 11.

ZITTRAIN, J. The Generative Internet. Harvard Law Review, roč. 119.

PRÁVNÍ PROBLÉMY KYBERNETICKÉ BEZPEČNOSTI

**doc. JUDr. Radim Polčák, Ph.D., JUDr. Jakub Harašta,
Mgr. Václav Stupka**

Vydala Masarykova univerzita
Žerotínovo nám. 617/9, 601 77 Brno

Spisy Právnické fakulty MU č. 576 (řada teoretická, Edice Scientia)

Tisk: Point CZ, s.r.o., Milady Horákové 890/20, 602 00 Brno
1. vydání, 2016

ISBN 978-80-210-8426-1
www.law.muni.cz