*Mgr. Roman Pačka*
*Národní centrum kybernetické bezpečnosti*
*Národní bezpečnostní úřad*

# Role státu v zajišťování kybernetické bezpečnosti[1]

## Úvod

Kyberprostor představuje rychle se vyvíjející prostředí, jehož jedinou konstantou je „změna". Každým dnem exponenciálně přibývá množství informací, dat a služeb v kyberprostoru. Občané jej stále více využívají, společnost jako celek je na něm den ode dne závislejší a ani stát již nemůže opomíjet veškeré výhody využívání kyberprostoru. Nicméně zvyšování počtu informací, dat a služeb v tomto digitálním prostředí spolu se zvyšováním závislosti na něm s sebou přináší i nárůst v počtu nových bezpečnostních hrozeb a zvyšování rizik. Již dávno tak státy a jejich vlády nemohou kyberprostor, respektive prostředí internetu ignorovat.

Fenomén provázanosti a vzrůstající závislosti na kyberprostoru přitom není nikterak škodlivý. Využívání kyberprostoru zvyšuje efektivitu a produktivitu všech odvětví lidské činnosti, státní správu nevyjímaje – stimuluje ekonomiku, zvyšuje konkurenceschopnost, apod. Na druhou stranu však otevřený charakter internetu a vystavování dat a informací v kyberprostoru snižuje nejen kybernetickou, ale i celkovou bezpečnost státu. Z tohoto důvodu se v posledních letech začaly státy stále více angažovat v oblasti zajišťování kybernetické bezpečnosti. V praxi se jedná především o přesun tradičních bezpečnostních aktivit na ochranu státu proti vnitřnímu i vnějšímu ohrožení do kyberprostoru, a také o ochranu svých vitálních funkcí před narušením či útokem z kyberprostoru, tj. ochranou své kritické informační infrastruktury (dále již jen „KII").

Tento článek si klade za cíl vytvořit základní přehled o roli státu v zajišťování kybernetické bezpečnosti a v tomto směru i vymezit působení bezpečnostních složek a institucí státu v kyberprostoru. Článek rovněž nabízí výčet (nikoliv vyčerpávající) jednotlivých metod, nástrojů a technik, které stát v tomto směru využívá a na jeho základě identifikuje problematické oblasti působení státních struktur v kyberprostoru. Z hlediska přínosu článku, zkoumané téma nebylo minimálně v českém prostředí nikterak souhrnně zpracováno a může tak sloužit akademické, ale i široké veřejnosti k pochopení proč a jakým způsobem stát v kyberprostoru figuruje. Lidem z bezpečnostní komunity pak pomůže s utvořením si komplexního obrazu o tom, jaké principy musí bezpečnostní složky státu dodržovat při zajišťování kybernetické bezpečnosti a jaká nezanedbatelná rizika a problematické oblasti toto atypické digitální prostředí přináší.

Co se struktury a logického členění textu týče, nejprve je představen teoretický rámec, v němž je vymezen termín kybernetické bezpečnosti spolu se základními funkcemi státu relevantními pro oblast kybernetické bezpečnosti. Dále je prezentován

[1] Tento příspěvek vychází ze zkušeností a praxe autora, který působí již několik let v rámci státních struktur zajišťujících kybernetickou bezpečnost jak na národní, tak i mezinárodní úrovni.

proces tvorby kybernetické bezpečnostní politiky na příkladu České republiky (dále již jen „ČR"). Stěžejní část článku se pak věnuje vymezení působnosti státu v kyberprostoru, respektive jeho činnostem, které jsou rozčleněny do čtyř částí: činnost policejních složek (vymáhání práva); činnost zpravodajských služeb; činnost vojenských složek (kybernetická obrana) a ochrana KII.

## Teoretický rámec: Stát a kybernetická bezpečnost

### *Kybernetická bezpečnost*

Bezpečnost jako taková představuje klíčový pojem bezpečnostní politiky každého státu. Definic bezpečnosti existuje celá řada a jejich význam je odvislý od konkrétního konceptuálního, teoretického a časového rámce, do něhož jsou zasazeny.[1] Neexistuje jednotná a všeobecně přijímaná definice bezpečnosti, nicméně v rámci české bezpečnostní komunity je poměrně široce přijímána definice Miroslava Mareše,[2] která popisuje *„bezpečnost jako stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizaci) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat."*

Kybernetická bezpečnost, jakožto podmnožina celkové bezpečnosti rovněž trpí absencí všeobecně přijímané definice. Každý si tak pod pojmem kybernetické bezpečnosti vybaví něco jiného a definice variuje i dle toho, s jakými aspekty kybernetické bezpečnosti se jedinec setkává. Nicméně ať už se zabýváme kybernetickou bezpečností průmyslových řídicích systémů, operačních systémů, cloudových úložišť, atd., bezpečnost zde pokaždé představuje připravenost služby či systému před útokem a jeho následky, spolu s plánováním obnovy funkčnosti při narušení. Na vysokém stupni abstrakce lze uvést tři obecné kategorie, neboli triády, které dohromady obsáhnou široký pojem kybernetické bezpečnosti:

a) předcházet, detekovat, reagovat,
b) lidé, procesy, technologie,
c) důvěrnost, integrita a dostupnost.[3]

Základem kybernetické bezpečnosti je snaha subjektu působit preventivně a předcházet tak jakémukoliv útoku či narušení. Nicméně subjekt si je vědom, že útok může být úspěšný a narušení může nastat, a proto se snaží veškeré kybernetické útoky a narušení detekovat a spolu s tím i plánovat co nejúčinnější reakci, která zahrnuje i plán obnovy na stav před útokem či narušením.

Druhá triáda poukazuje na provázanost a nerozdělitelnost složek kybernetické bezpečnosti. V tomto smyslu veškeré systémy v kyberprostoru potřebují lidský

[1] Viz FRANK, Libor. Analýza a predikce bezpečnostních hrozeb a rizik v České republice. Disertační práce. Brno: FSS MU, 2006, s. 11.
[2] Viz MAREŠ, Miroslav. Bezpečnost. In: ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů.* Brno: Vojenská akademie v Brně, 2002, s. 13 [online]. [cit. 2015-06-10]. Dostupný z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.
[3] Viz BAYUK, Jennifer L. (et al.). *Cyber security policy guidebook.* Hoboken: John Wiley, 2012, s. 2-3. ISBN 978-1-118-02780-6.
Viz PURPURA, Philip. *Security and Loss Prevention: An Introduction.* San Diego: Butterworth-Heinemann, 2007, s. 17-18. ISBN 978-0-08-055400-6.





element, tedy správce a operátory, kteří musí dodržovat stanovené bezpečnostní procesy ve smyslu zajišťování kybernetické bezpečnosti. Tyto procesy však logicky vyžadují technologická řešení a ani jedna z těchto tří složek tak nemůže fungovat samostatně, tj. bez ostatních dvou.

Poslední trojice se vztahuje především k obsahu, respektive k informacím a datům uvnitř chráněných systémů a služeb a bývá označována jako esenciální součást kybernetické bezpečnosti (tzv. CIA triáda, z angl. *confidentiality, integrity, availability*).[1] Důvěrnost zde znamená, že přístup k informacím a datům mají vždy pouze autorizované osoby, neboli informace a data nejsou odhaleny nebo dostupné neoprávněným osobám. Integrita představuje nezměnitelnost, platnost a přesnost těchto informací a dat, která mohou modifikovat pouze autorizovaní. A konečně dostupnost vyjadřuje přístupnost k těmto informacím a datům a míru použitelnosti autorizovanými osobami. V kontextu zajišťování kybernetické bezpečnosti pak musí být hledán vyvážený přístup mezi všemi složkami této trojice vzhledem k chráněnému objektu.

Závěrem, pokud tyto tři kategorie spojíme, tak lze jednoduše vyvodit, že kybernetická bezpečnost představuje efektivní využívání lidí, procesů a technologií k prevenci, detekci a reakci na kybernetické útoky či narušení kyberprostoru, které by způsobily škodu v důvěrnosti, integritě nebo dostupnosti informací či dat v kyberprostoru.

### *Funkce státu vzhledem k zajišťování kybernetické bezpečnosti*

Aby stát mohl správným způsobem kybernetickou bezpečnost zajišťovat, musí být vymezena jeho funkce, působnost a rozsah aktivit v této oblasti.

V obecné rovině patří mezi hlavní funkce státu funkce vnitřní (právní, bezpečnostní, hospodářská, sociální, kulturní) a funkce vnější (obranná, hospodářská, styky s ostatními státy).[2] Na základě obsahu těchto funkcí musí stát z hlediska právní funkce regulovat a zakotvit vztahy mezi relevantními subjekty kybernetické bezpečnosti spolu se svými aktivitami, které v oblasti kybernetické bezpečnosti provádí. Dále musí stát logicky zastávat funkci bezpečnostní a obrannou, tedy chránit společnost zastoupenou ve státě, respektive obyvatele státu před všemi vnějšími i vnitřními kybernetickými hrozbami, útoky či jinými narušeními kyberprostoru s negativním dopadem na společnost, potažmo stát. Kvůli absenci geografických hranic v kyberprostoru stát musí vytvářet spojenectví a budovat důvěru s ostatními státy světa za účelem prosazování svých národních zájmů v digitálním prostředí. A v neposlední řadě by měl stát plnit i funkci kulturní ve smyslu prosazování kultury informační společnosti pomocí zajištění svobodného přístupu ke všem službám informační společnosti.

#### *Tvorba kybernetické bezpečnostní politiky*

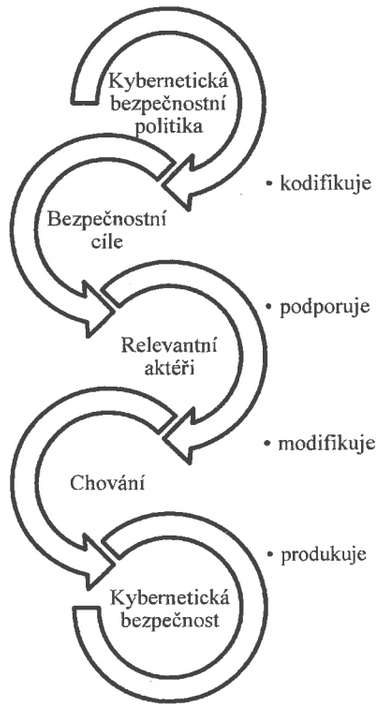
Při zajišťování kybernetické bezpečnosti a za účelem plnění všech vnitřních i vnějších funkcí si musí každý stát stanovit kybernetickou bezpečnostní politiku. Tato

[1] Viz HARRIS, Shon. CISSP All-In-One Exam Guide. Columbus: McGraw-Hill, 2013, s. 22-24. ISBN 978-0-07-178173-2.
[2] Viz SMOLÍK, Josef. Úvod do studia mezinárodních vztahů. Praha: Grada Publishing, 2014, s. 60. ISBN 978-80-247-5131-3.

politika, stejně jako celková bezpečnostní politika, reprezentuje politickou koncepci a soubor všech státních opatření k zajištění vnitřní a vnější bezpečnosti státu,[1] tentokráte však v kyberprostoru. Kybernetickou bezpečnostní politiku stát veřejně deklaruje, a to skrze potřebné legislativní, strategické a další koncepční dokumenty.

Nejlépe logiku a proces tvorby kybernetické bezpečnostní politiky popisuje Bayuk[2] v rámci tohoto grafu (obrázek č. 1), který je zde demonstrován na případu České republiky:

Obrázek č. 1: Proces tvorby kybernetické bezpečnostní politiky




Kybernetická bezpečnostní politika je stejně jako ostatní bezpečnostní politiky vytvářená a navrhovaná některým ze zodpovědných vládních těles[3] a přijímána

[1] Viz FRANK, Libor. Bezpečnostní politika. In: ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů.* Brno: Vojenská akademie v Brně, 2002, s. 82 [online]. [cit. 2015-06-10]. Dostupný z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.

[2] Viz BAYUK, Jennifer L. (et al.). *Cyber security policy guidebook.* Hoboken: John Wiley, 2012, s. 4. ISBN 978-1-118-02780-6.

[3] V České republice se jedná především o Národní bezpečnostní úřad, který působí jako gestor kybernetické bezpečnosti a národní autorita v této oblasti (dle usnesení vlády ČR č. 781/2011) a vykonává státní správu v oblasti kybernetické bezpečnosti (viz zákon č. 181/2014 Sb.).





samotnou vládou státu. Vláda skrze schválení a tedy i nastavení kybernetické bezpečnostní politiky kodifikuje své bezpečnostní cíle v kybernetické oblasti (např. pomocí zákonů, vyhlášek, národní strategií, apod.),[1] a tím podporuje či zavazuje (v případě dokumentů legislativního charakteru) všechny relevantní aktéry[2] v tom, aby stanovené bezpečnostní cíle dodržovali. Tímto se změní chování všech relevantních subjektů participujících na zajišťování kybernetické bezpečnosti ve státě, kybernetická bezpečnostní politika se tak realizuje a požadovaná kybernetická bezpečnost je zajištěna.

### *Působnost státu v zajišťování kybernetické bezpečnosti*

Způsob fungování vlád v dnešním světě je stále odrazem let minulých a stát má proto zákonitě problémy vyrovnávat se s novými bezpečnostními výzvami, které dnešní svět přináší. Jedná se nejen o výzvy, které přináší kyberprostor, ale i výzvy v podobě terorismu, globální finanční krize, či změny klimatu, apod.[3] Výzvy vzešlé z kyberprostoru jsou však oproti zbylým jmenovaným zcela unikátní a zavést bezpečnostní politiku pro tuto oblast je kvůli z velké části nefyzickému, digitálnímu charakteru prostředí velmi obtížné. Aplikovat tak tradiční vládní postupy přijímání legislativních a jiných opatření pro zabezpečení neustále se vyvíjejícího se kyberprostoru je v dostatečně efektivní míře nelehké.

Z tohoto důvodu stát jednoduše není schopen dostatečně rychle měnit svou kybernetickou bezpečnostní politiku skrze kodifikaci stále nových bezpečnostních cílů. Jediným východiskem z této situace tak pro stát představuje nastavení své kybernetické bezpečnostní politiky tak, aby byla dostatečně pružná, avšak stále dostatečně účinná, což sebou přináší mnoho problematických oblastí. Stát tudíž musí zaměřit své úsilí v této oblasti na budování účinného, komplexního přístupu k zajišťování kybernetické bezpečnosti, který bude za všech okolností legální, a celkově pak musí být prostoupen všemi aktivitami, které stát v kyberprostoru provádí.

## Základní aktivity státu v rámci zajišťování kybernetické bezpečnosti

Stát, respektive jeho bezpečnostní složky a instituce působí v kyberprostoru v rámci čtyř základních oblastí, kterými jsou:

[1] Kybernetická bezpečnostní politika je v ČR kodifikována zejména skrze: Bezpečnostní strategii ČR; Národní strategii kybernetické bezpečnosti ČR pro období let od 2015 až 2020 (dále již jen „NSKB 2015-2020") a Akční plán národní strategie kybernetické bezpečnosti ČR pro období let od 2015 až 2020 (dále již jen „AP 2015-2020"); zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (tzv. Zákon o kybernetické bezpečnosti) a vyhlášku o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (tzv. Vyhláška o kybernetické bezpečnosti) a vyhlášku o významných informačních systémech a jejich určujících kritériích.

[2] Zákon o kybernetické bezpečnosti v ČR reguluje především subjekty státní správy a soukromé subjekty vlastnící či spravující prvky kritické informační infrastruktury, a tím modifikuje chování relevantních aktérů směrem k zajištění vyšší kybernetické bezpečnosti státu.

[3] Viz FRIEDMAN, Allan a SINGER, W., Peter. *Cybersecurity and cyberwar. What everyone needs to know.* New York: Oxford University Press, 2014, s. 193-194. ISBN 978-0-19-991811-9.

1. činnost policejních složek (vymáhání práva)
2. činnost zpravodajských služeb,
3. činnost vojenských složek (kybernetická obrana),
4. a ochrana KII.

***Činnost policejních složek (vymáhání práva)***

Zajistit vnitřní bezpečnost je jedna ze základních funkcí států, která z velké části spočívá ve vymáhání práva (z angl. *law enforcement*), tedy potírání kriminality a ochraně společnosti před trestnou činností. Právo je však nyní potřeba vymáhat nejen ve fyzickém světě, ale i v kyberprostoru. Zločinci se celosvětově velmi rychle adaptovali na nové virtuální prostředí a většina států světa by tak již měla být schopna řešit případy informační kriminality a disponovat potřebným vybavením a schopnostmi pro potírání informačních zločinů.

Definici informační kriminality nabízí například Jirásek, Novák a Požár,[1] podle nichž je informační kriminalita: *„Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat."*

Každý stát přitom prosazuje svou vlastní právní úpravu v oblasti informační kriminality a tím i určuje, které činy považuje za trestné a které nikoliv. Informační kriminalita je pak ve velké míře páchána ze zahraničí, tj. většinou z území států, které mají odlišné vnímání v oblasti informační kriminality a odlišnou právní úpravu, což ztěžuje státu vykonávat svou bezpečnostní funkci.

Nicméně obecně platí, že stát se vzhledem k trendu digitalizace (digitalizace fotek, korespondence, knih, atd.) musí vždy vypořádávat s velkým množstvím dat, respektive důkazních materiálů.[2] Základní metodou jakým způsobem zkoumat tato data a informace pak představuje metoda digitální forenzní analýzy, kterou si musí osvojit všechna policejní specializovaná pracoviště. Hlavní cíl této metody spočívá v použití analytických technik ke sběru a shromáždění všech důkazů z digitálního prostředí o trestném činu, které by mohly být použity u soudního procesu. Digitální forenzní analýza přitom vyžaduje kombinaci technických dovedností, právní prozíravosti a etického jednání. Představuje tedy zásadní disciplínu, která má sílu bránit rozmachu informační kriminality a rozvoj této metody příslušnými složkami státu má své opodstatnění i v rámci prevence informační kriminality.[3]

[1] Viz JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie České republiky, 2015, s. 55-56. ISBN 978-80-7251-436-6.

[2] Viz BAGGILI, Ibrahim a BREITINGER, Frank. Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer. In: *Sociotechnical Behavior Mining: From Data to Decisions*? Papers from the 2015 AAAI Spring Symposium, 2015, s. 6 [online]. [cit. 2015-06-10]. Dostupný z: http://www.aaai.org/ocs/index.php/SSS/SSS15/paper/viewFile/10227/10092. Viz SOLOMON, Michael, BARRETT, Diane a BROOM, Neil. *Computer Forensics Jump Start*. San Francisco: Sybex, 2005, s. 11. ISBN 978-0-470-93166-0.

[3] Viz BASSETT, Richard, BASS, Linda a O'BRIEN, Paul. Computer forensics: An essential ingredient for cyber security. In: *Journal of science and technology*. Vol. 3, No. 1, 2016, s. 22. ISSN: 1545-0287.





S rozmachem používání internetu a ICT se nejen pro účely vyšetřování informační kriminality začal v rámci potírání nejrůznějších druhů kriminality používat ve velké míře i OSINT (z angl. *Open Source INTelligence*), tj. zpravodajství z otevřených, většinou internetových, zdrojů. Internet díky svému otevřenému charakteru slouží jako obrovský, užitečný zdroj nejrůznějších dat, která mohou být relevantní pro vyšetřování trestných činů či jejich předcházení.[1]

Sbírat a analyzovat otevřená data a informace je v obecné rovině právně nezávadné, avšak stát občas využívá i data, která nejsou volně přístupná třetí straně – např. data z komunikace na internetu relevantní k vyšetřování trestních činů. Technika sběru těchto dat se nazývá *wiretapping* (odposlouchávání) a představuje problematickou oblast hned ve dvou rovinách – legální a technické.[2] Z právního hlediska se při takovém odposlouchávání vždy zasahuje do práv a soukromí druhých osob, a proto by státní složky vymáhající právo měly stejně jako ve fyzickém světě disponovat vždy soudním či jiným legálním povolením. Stát by tedy měl definovat kdy a za jakých podmínek může být komunikace odposlouchávána. Z technického pohledu je pak otázkou, jakým způsobem odposlech provádět a zdali vůbec státní (mnohdy podfinancované) specializované policejní jednotky disponují potřebným technickým vybavením a schopnostmi tuto aktivitu provádět. Zmínit můžeme například problém při odposlechu asi nejznámější internetové komunikační služby *Skype*. Skype se vyznačuje používáním peer-to-peer technologie, která oproti tradičnímu řešení komunikace skrze klient-server má mnoho výhod pro uživatele (např. snižuje riziko selhání funkčnosti sítě a navyšuje kvalitu hovorů), avšak pro policejní složky architektura distribuované komunikace, bez jediného centrálního uzlu představuje velký technický problém jak odposlech provádět. Neexistuje zde totiž jediné místo, skrze které by mohly policejní složky odposlouchávat potřebnou komunikaci a zprávy z této komunikace byly dostupné v ucelené podobě.

Potírání informační kriminality státem v neposlední řadě ztěžují i lehce dostupné, jednoduché anonymizační nástroje,[3] které může využít téměř každý alespoň trochu ICT znalý uživatel či zločinec.[4] A zároveň je nutno upozornit i na problém teritoriality. Stát má vymezenou svou působnost, respektive vymahatelnost práva, svými geografickými hranicemi. Kyberprostor stírající tyto hranice a jurisdikční nejednotnost v oblasti informační kriminality napříč státy pak silně omezuje tradiční roli státu při vymáhání práva.

[1] BRAVO, Rogerio. Open sources in cybercrime investigation: concept and implications, 2014, s. 3 [online]. [cit. 2015-06-10]. Dostupný z: http://www.academia.edu/7301278/OPEN_SOURCES_IN_CYBERCRIME_INVESTIGATION_concept_and_implications.

[2] Viz ROSENZWEIG, Paul. The Evolution of Wiretapping. In: *Criminal Law & Procedure*. Volume 12, Issue 2, 2011 [online]. [cit. 2015-06-10]. Dostupný z: http://www.fed-soc.org/library/doclib/20110912_RosenzweigEngage12.2.pdf.

[3] Konkrétně můžeme zmínit například použití proxy serverů, či známou anonymizační síť TOR, jejíž použití je opravdu jednoduché a riziko zjištění identity uživatele je s jejím využitím minimální.

[4] Tyto anonymizační nástroje a metody se nepoužívají pouze k páchání trestné činnosti na internetu a jejich používání je legální.

### *Činnost zpravodajských služeb*

Většina lidí považuje zpravodajskou činnost za nezbytnou pro chod státu. Vlády jsou díky ní dostatečně informovány a mohou tak činit rozumné kroky.[1] Zpravodajská, či špionážní činnost je také někdy nazývána „druhou nejstarší profesí" a její základy nalezneme již tisíce let zpátky v učení čínského vojenského stratéga Sun-Tzu nebo indického Čánakja.[2] A v podstatě až do nástupu éry masivního využívání internetu nepředstavovaly zpravodajské aktivity, potažmo akty špionáže, tak komplexní problém jako nyní. Pokud státy chtěly odposlouchávat například vojenskou komunikaci druhých států, tak na jejich vojenské sítě nasadily zpravodajskou techniku a odposlouchávaly pouze vojenskou komunikaci. V dnešní době však veškerá, vojenská i soukromá komunikace probíhá na jedné síti – internetu, což přináší na jednu stranu mnoho výhod pro zpravodajské služby, ale zároveň i mnoho povinností a omezení pro stát.

Kyberprostor a globální závislost společnosti na internetu a ICT prostředcích poskytuje zpravodajským službám široké možnosti jak z území svého státu vykonávat svou činnost a v jejím rámci i kybernetickou špionáž. Výkladový slovník kybernetické bezpečnosti definuje kybernetickou špionáž jako: *„Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy."*[3] Nehledě na fakt, zdali špionáž probíhá ve fyzickém či digitálním prostředí, hlavní motivace se nemění – preemptivně působit a odhalovat co nejvíce bezpečnostních hrozeb a simultánně udržovat veškerá státní tajemství v bezpečí. Samotnou špionáž pak můžeme rozdělit dle cílového objektu na dvě skupiny:[4]

1. špionáž proti státním aktérům,
2. průmyslová špionáž,
3. špionáž proti obyvatelstvu.

Kybernetická špionáž směrem do zahraničí proti státním subjektům či průmyslová špionáž není veřejně přiznávána, ba spíše naopak – odsuzována.[5] Na druhou stranu je však rozumné předpokládat, že mnoho zemí disponuje potřebnými schopnostmi a kapacitami k výkonu těchto zpravodajských činností v kyberprostoru, potažmo kybernetické špionáže, a takové aktivity v praxi běžně probíhají.[6] V rámci všech druhů špionáže pak vyvstává otázka legálnosti takového jednání jak z pohledu

[1] DETERMANN, Lothar a GUTTENBERG, Karl T. On War and Peace in Cyberspace. In: *Hastings constitutional law quarterly*. Summer. Vol. 41, No. 4, 2014, s. 880 [online]. [cit. 2015-06-10]. Dostupný z: http://www.hastingsconlawquarterly.org/archives/V41/I4/Determann_Online.pdf.
[2] Viz CHESTERMAN, S. The Spy Who Came in from the Cold War: Intelligence and International Law. In: *Michigan Journal of International Law*. Vol. 27, 2006, s. 1072. ISSN 1052-2867.
[3] Viz JIRÁSEK, Petr, NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie České republiky, 2015, s. 70. ISBN 978-80-7251-436-6.
[4] Viz SCHNEIER, Bruce. *Data and Goliath*. New York: Norton, 2014, s. 75. ISBN 978-0-393-24481-6.
[5] Viz Ibid, s. 72.
[6] Viz Ibid, s. 74.
Viz DETERMANN, Lothar a GUTTENBERG, Karl, T., 2014, s. 881.





národních právních úprav, tak z pohledu mezinárodního práva, kde kybernetická špionáž představuje velmi problematickou oblast.[1]

I když připustíme, že kybernetická špionáž reálně probíhá a zpravodajské služby jsou velice aktivní v kyberprostoru, veřejné informace, jakými schopnostmi a možnostmi v kyberprostoru disponují, jsou nedostupné. Nicméně událost z roku 2013, kdy Edward Snowden[2] odhalil údajné projekty a rozsah zpravodajských aktivit USA v kyberprostoru, umožnila veřejnosti vytvořit si představu, jakým směrem se ubírají a jakými možnostmi a schopnostmi zpravodajské služby mohou v dnešní době disponovat (za vynaložení dostatečných finančních a jiných nákladů a politické vůle).

K plnění svých cílů zpravodajské služby využívají nejspíše podobných metod a technik zmíněných v kapitole 2.1 a musí se vypořádat s podobnými technickými, právními, anonymizačními i teritoriálními otázkami. Nicméně jejich rozsah činností se značně rozšiřuje, a tím i více komplikuje. Internetové prostředí umožňuje namísto sběru informací a dat o jednotlivých podezřelých subjektech sbírat i údaje a zachycovat komunikaci o celé společnosti, tj. plošně. Kombinace cíleného a plošného způsobu získávání dat a informací pak lépe odpovídá profilu a úkolům zpravodajských služeb, které necílí pouze na jednotlivé subjekty, které již zločin spáchaly. Zpravodajské služby musí působit především preemptivně, a proto by měly mít logicky širší záběr nežli policejní složky reagující vždy *ex post* na jednotlivé případy informační kriminality.

Konkrétně za využití zadních vrátek (z angl. *backdoors*) či skrze nasazení špionážního škodlivého software (z angl. *malware*) k přístupu do požadovaného systému nebo skrze nejrůznější automatizované nástroje mohou zpravodajské služby extrahovat důležité informace o zájmových subjektech, mapovat mezi nimi vztahy, identifikovat nové hrozby, lépe kvantifikovat bezpečnostní rizika, apod. Konkrétně k plošné analýze velkého množství dat z kyberprostoru je používána především automatizovaná technika *data mining* (vytěžování či dolování dat).

Data mining v obecném slova smyslu zahrnuje vytěžování obrovského množství dat (tzv. *big data*) a aplikaci vybraných analytických metod pro vyhledávání zajímavých vztahů v těchto datech.[3] Data mining pak zpravodajské služby mohou využívat v rámci vyhledávání nových bezpečnostních hrozeb, trendů, zájmových osob či skupin, apod.

Dvěma primárními cíli data mining v praxi jsou:

– predikce – umožňuje předvídat budoucí hodnoty atributů na základě nalezených vzorů v datech;

[1] Srov. DETERMANN, Lothar a GUTTENBERG, Karl T., 2014; RADSAN, John A. The Unresolved Equation of Espionage and International law. In: Michigan Journal of International Law, Vol. 28, No. 597, 2007. ISSN: 1052-2867;
DEMAREST, Geoffrey B. Espionage in International Law. In: Denver Journal of International Law and Policy. Vol. 24, 1996. ISSN: 0196-2035.
[2] Edward Snowden je bývalý spolupracovník amerických tajných služeb. Do června 2013 pracoval pro společnost Booz Allen Hamilton úzce spolupracující s těmito službami. Viz GUARDIAN. Booz Allen Hamilton: Edward Snowden's US contracting firm, 2013 [online]. [cit. 2015-06-10]. Dostupný z: http://www.theguardian.com/world/2013/jun/09/boozallen-hamilton-edward-snowden) .
[3] Viz BERKA, Petr. *Dobývání znalostí z databází*. Praha: Academia, 2003, s. 18. ISBN 80-200-1062-9.

– deskripce – popisuje nalezené vzory a vztahy v datech.[1]

Na druhou stranu však plošný sběr dat a využívání data mining zpravodajskými službami představuje finančně náročnou položku pro stát. Někteří experti[2] pak poukazují i na nedostatečnou efektivitu těchto technik, zbytečné zasahování do práv a svobod „nevinného" obyvatelstva, a apelují proto na upuštění zpravodajských aktivit od masivního, plošného sledování směrem k minimalizaci, tj. osvědčenému, cílenému sledování.

***Činnost vojenských složek (kybernetická obrana)***

O kyberprostoru se již několik let hovoří jako o tzv. „pátém bojišti".[3] Nárůst zájmu o problematiku kybernetického bojiště a hrozbu kybernetické války se dá pozorovat zejména od roku 2007, kdy proběhly rozsáhlé kybernetické útoky na Estonsko. V poslední době pak v souvislosti s ruským obsazením ukrajinského poloostrova Krym, kdy se na obou stranách konfliktu událo velké množství kybernetických incidentů, je možno identifikovat i současnou tendenci využívání kyberprostoru pro vojenské účely. Lze tedy predikovat, že vojenské operace v kyberprostoru se stanou v budoucnosti nedílnou součástí většiny konvenčních ozbrojených konfliktů a napříč státy světa proto můžeme pozorovat trend budování vojenských obranných kapacit státu v kyberprostoru.[4]

Co se týče kybernetické obrany, opět neexistuje žádná ustálená definice, ale obecně se jí rozumí schopnost a možnost státu působit aktivně v kyberprostoru za využití potřebných technologických a znalostních kapacit ve směru eliminace, potlačení či předcházení závažných kybernetických útoků, které mohou přicházet jak ze zahraniční, tak z vnitrostátní úrovně. Vzhledem k nutnosti specializovaného pracoviště působit jak interně, tak externě a zároveň mít i blízký vztah s vojenskými složkami země, je většinou určeno, aby kybernetickou obranu zajišťovaly specializované složky uvnitř ozbrojených sil státu – armády.[5]

Jako jeden z prvních, který upozornil na nutnost přijetí aktivního pojetí kybernetické obrany, byl Chris Neitzert, který ve svém příspěvku „Guerilla Anti-

[1] Viz FAYYAD, Usama M., PIATETSKY-SHAPIRO, Gregory a SMYTH, Padhraic. From data mining to knowledge discovery in databases, 1996 [online]. [cit. 2015-06-10]. Dostupný z: http://www.csd.uwo.ca/faculty/ling/cs435/fayyad.pdf.

[2] SCHNEIER, Bruce. 2014, s. 140.

[3] Viz HEALEY, Jason a WILSON, A. J. Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain, 2013, s. 53 [online]. [cit. 2015-06-10]. Dostupný z: http://mercury.ethz.ch/serviceengine/Files/ISN/160116/ipublicationdocument_singledocument/2a41383f-8970-4c32-9193-845067598ece/en/bsc130221cyberwprpub.pdf.
Viz MCGUFFIN, Chris. On domains: Cyber and the practice of warfare. In: International Journal: Canada's Journal of Global Policy Analysis, Vol. 69, No. 3, 2014. ISSN 0020-7020.

[4] Tento trend ostatně reflektuje i ČR, která si v rámci své nově přijaté NSKB 2015-2020 a souvisejícím AP 2015-2020 stanovila v nejbližších letech vybudovat „Národní centrum kybernetických sil", které bude zajišťovat kybernetickou obranu země. ČR tak bude v budoucnu disponovat tělesem schopným plnit široké spektrum vojenských činností v kyberprostoru, které zajišťování kybernetické obrany obnáší.

[5] Např. USA, Rusko, Čína, Izrael, Indie, Brazílie, Nový Zéland, a další. Viz SCHNEIER, Bruce. 2014, s. 74.





Penetration Tactics" z roku 2003 prohlásil, že veškerou informační bezpečnost pokládá za formu bojiště, kde útočník bývá neviděn, cítí se nedotknutelný a má tak jen velmi malý strach z odezvy či následků svého jednání. Již tehdy Neitzert kritizoval bezpečnostní praktiky založené na strategii reakce až následně po útoku, které využívají postupu *„penetrate and patch"*, kdy se po narušení systému daný systém na základě daného útoku začne chránit. Toto označoval za nedostatečné, neboť systémy již nijak blíže neřeší budoucí útoky, které budou zase zcela odlišné od těch, které již systém narušily.[1] Ostatně samotný termín „guerilla" v názvu odráží současné pojetí kyberprostoru, které připomíná asymetrické, guerillové bojiště. Proto například americký generál James Cartwright prohlásil v roce 2012, že je zapotřebí tuto situaci změnit, začít otevřeněji hovořit o státních útočných kapacitách v kyberprostoru, pracovat na nich a učinit je důvěryhodnými pro veřejnost, aby občané věděli, že za kybernetické útoky, stejně jako za kinetické útoky následuje trest.[2] V roce 2015 pak již můžeme konstatovat, že použití konceptu aktivní kybernetické obrany začalo být širokou veřejností akceptováno a státy se vlastnictvím těchto kapacit netají.

Metody, nástroje a techniky zajišťování kybernetické obrany se však liší v závislosti na pojetí kybernetické obrany konkrétním státem. Obecně bychom mohli uvést tři základní rysy aktivní obrany:[3]

1. Zajišťování kybernetické obrany v reálném čase (schopnost reagovat efektivně a dostatečně rychle)
2. Schopnost aktivní identifikace a rekognoskace nepřítele v kyberprostoru (spočívá v lokálním i vzdáleném shromažďování informací, tj. zisk logů či dat ze síťového provozu; OSINT; monitoring zranitelností, aj.)
3. Schopnost provádět odvetné (tzv. *hacking back* nebo *striking back*) i preemptivní kybernetické útoky (např. nasazení malware, modifikace síťového provozu, provádění DoS/DDoS útoků proti útočníkovi, apod.)

Nicméně nežli se přistoupí k jakýmkoliv ofenzivním taktikám kybernetické obrany, je třeba vyčerpat všechny ostatní možnosti, tj. defenzivní možnosti kybernetické

[1] Viz SVFORUM. Security SIG: Guerilla anti-penetration tactics, 2003 [online]. [cit. 2015-06-10]. Dostupný z: https://svforum.org/Software-Architecture-and-Platform/Security-SIG-Guerilla-Anti-Penetration-Tactics.

[2] Viz LIMNÉLL, Jarno. Offensive cyber capabilities are needed because of deterrence. In: RANTAPELKONEN, Jari a SALMINEN, Mirva. (eds.): The fog of cyber defence. Tampere: National defence university, 2013. ISBN 978-951-25-2430-3.

[3] Viz DUVENAGE, Petrus a SOLMS, Sebastian von. Putting Counterintelligence in Cyber Counterintelligence: Back to the Future, 2014. In: LIAROPOULOS, A. – TSIHRINTZIS (eds.). Proceedings of the 13th European Conference on Cyber Warfare and Security ECCWS-2014. Reading: Academic Conferences and Publishing International Limited. ISBN 978-1-910309-25-4. Viz PAČKA, Roman. Difference Between Cyber Security and Cyber Defence from a Czech Perspective. In: Cyber Security Review, Spring ed., London: Delta Business, 2015. pp. 20-24. ISSN 2055-6950.
Viz WESTBY, Jody. Caution: Active response to cyber attacks has high risk, 2013 [online]. [cit. 2015-06-10]. Dostupný z: http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

bezpečnosti.[1] Prostředky kybernetické obrany tak slouží jako prostředky poslední instance.

Kybernetické útoky, které může být nutné řešit v rovině kybernetické obrany, se liší v návaznosti na pojetí kybernetické bezpečnosti a kybernetické obrany daného státu. Obecně však představují, například z pohledu České republiky, jakékoliv závažné kybernetické útoky, které:[2]

1. ovlivňují obranyschopnost země, či řízení a koordinaci vojenských sil nebo představují vysoké riziko pro bezpečnost státu, které již nelze zvládat pomocí prostředků kybernetické bezpečnosti;
2. jsou považovány za cílené / prováděné „na míru" a mají závažné konsekvence vůči stavu bezpečnosti v zemi či negativní vliv na strategická aktiva a národní zájmy země (např. případy typu Hydraq, Stuxnet nebo jiné APT);
3. probíhají v masivním měřítku a nelze je zvládnout běžnými prostředky, tj. po vyčerpání standardních opatření a nástrojů složek kybernetické bezpečnosti (např. DDoS útoky v Estonsku 2007);
4. mají zničující efekt na kritická aktiva země a bezpečnost obyvatelstva (např. závažné kybernetické útoky na průmyslové řídicí systémy/SCADA v rámci KII).

Vzhledem k ofenzivnímu charakteru této činnosti pak stát nesmí, stejně jako v případě provádění zpravodajské činnosti v kyberprostoru, opomíjet potřebu zákonného zmocnění či ochrany práv a svobod obyvatel. Akce aktivní obrany logicky zasahují do práv druhých, z hlediska vnitrostátního i mezinárodního práva mohou být opět problematické a logicky je toto téma i politicky citlivé. Stát proto musí vždy jasně zakotvit své aktivity v rámci kybernetické obrany do svého právního řádu.

***Ochrana kritické informační infrastruktury***

Již v roce 1948 Hans Morgenthau[3] napsal: *„…národní bezpečnost závisí na integritě státních hranic a institucí."*, což platí dodnes. V kyberprostoru se však geografické hranice lehce stírají a tak národní bezpečnost a chod státu závisí již jen na integritě a bezpečnosti státních a jiných kritických institucí.

Současná infrastruktura států je od dodávek elektřiny až po volby do parlamentu digitalizovaná a připojená k internetu. Stát, potažmo jeho vláda jako tvůrce bezpečnostní politiky státu, se tím pádem musí obávat hrozby nejen fyzických, ale i kybernetických útoků na svou kritickou infrastrukturu, respektive na podmnožinu kritické infrastruktury svázanou s kyberprostorem a ICT – KII.

Definice a proces určování KIi se opět země od země liší, v ČR představuje: *„Komplex informačních a komunikačních systémů (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti), jejichž nefunkčnost by*

[1] Viz LIMNÉLL, Jarno. Controversial active cyber defense, 2012 [online]. [cit. 2015-06-10]. Dostupný z: http://www.infosecisland.com/blogview/22757-Controversial-Active-Cyber-Defense.html.
Viz PAČKA, Roman, 2015, s. 22-23.
[2] Ibid., s. 23.
[3] Viz MORGENTHAU, Hans J. *Politics among nations: the struggle for power and peace*. New York: Knopf, 1948. bez ISBN.

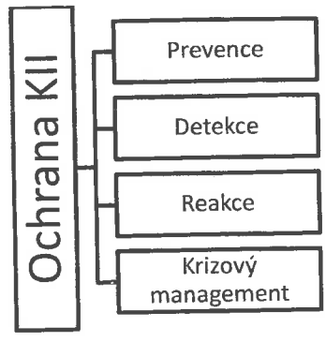




*mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu."*[1]

Problematika ochrany KII je přitom nesmírně širokou a nákladnou oblastí, která vyžaduje multisektorální řešení, vyváženou strategii státu a prioritizaci.[2] Na obecné úrovni se ochrana KII skládá ze čtyř pilířů (obrázek č. 2), které definují, jakou roli by měl v této oblasti stát zaujmout:[3]

Obrázek č. 2: Čtyři pilíře ochrany KII




„Prevence" se zaměřuje na zajišťování kybernetické bezpečnosti KII státu tak, aby byla co nejméně zranitelná vůči jakémukoliv narušení a aby byly všechny relevantní subjekty v rámci KII schopny a připraveny na možnost výskytu kybernetických bezpečnostních incidentů.

„Detekce" představuje schopnost státu co nejrychleji detekovat nové kybernetické hrozby, útoky a nastalé kybernetické bezpečnostní incidenty. K tomuto účelu slouží především pracoviště typu CERT/CSIRT,[4] jejichž hlavní úloha spočívá ve sdílení na národní a mezinárodní úrovni technických i netechnických informací o hrozbách, zranitelnostech, útocích, apod. S potřebou „detekce" i „reakce" na kybernetické bezpečnostní incidenty tedy stát v rámci ochrany KII ve většině případů zřizuje svůj vrcholový („vládní" či „národní") CERT/CSIRT,[5] který je za tuto oblast zodpovědný. Tento subjekt pak z hlediska své tzv. *„constituency"*,[6] která většinou zahrnuje subjekty KII a další subjekty spravující vitální infrastrukturu státu, nutně

[1] Viz JIRÁSEK, Petr, NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie České republiky, 2015, s. 65-66. ISBN 978-80-7251-436-6.
[2] Viz EDWARDS, M. (ed.). Critical Infrastructure Protection. Amsterdam: IOS Press BV, 2014, s. v. ISBN 978-1-61499-356-8.
[3] Viz SUTER, Manuel. A generic national framework for critical information infrastructure protection (CIIP). Zurich: ITU, 2007, s. 2-4 [online]. [cit. 2015-06-10]. Dostupný z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
[4] *Computer Emergency Response Team* nebo *Computer Security Incident Response Team*, tj. koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty incidenty.
[5] V ČR působí v rámci ochrany KII vládní CERT, tzv. „GovCERT.CZ".
[6] Rozsah působnosti, respektive výčet subjektů spadající do kompetence daného CERT/CSIRT.

propojuje výše zmíněné 3 oblasti (kapitola 2.1 – 2.3) a slouží jako informační a koordinační hub pro celkovou kybernetickou bezpečnost ve státě. Vrcholové pracoviště CERT/CSIRT tak musí disponovat alespoň omezeným přístupem k informacím od subjektů zodpovědných za informační kriminalitu (tj. policejních složek), za zpravodajskou činnost v kyberprostoru (tj. zpravodajské služby) a za kybernetickou obranu (tj. specializované armádní složky). Pouze za předpokladu propojení veškerých relevantních informací od těchto subjektů, dokáže vrcholové pracoviště typu CERT/CSIRT včas detekovat a efektivně sdílet a distribuovat informace o ohrožení relevantním subjektům KII a přijímat účinná protiopatření.

„Reakce" zahrnuje identifikaci a nápravu příčin narušení kyberprostoru, respektive kybernetických bezpečnostních incidentů. Vrcholový CERT/CSIRT v této fázi poskytuje postiženým subjektům KII technickou podporu a pomoc s řešením nastalé situace. Vrcholový CERT/CSIRT však nesupluje krizový management a přímé řešení narušení kyberprostoru u postiženého subjektu, má tento proces pouze doplnit. V rámci ochrany KII tedy poskytuje především rady a vedení při zvládání jednotlivých incidentů, spíše nežli poskytování kompletního procesu řešení situace. Jelikož poškození a dopad kybernetických útoků závisí ve velké míře na délce trvání útoku, musí vrcholový CERT/CSIRT i postižený subjekt reagovat co nejdříve a co nejefektivněji. V neposlední řadě pak fáze „reakce" zahrnuje i *ex post* analýzu kybernetických bezpečnostních incidentů. Ve spolupráci s postiženým subjektem by tak vrcholový CERT/CSIRT měl analyzovat (např. pomocí metod reverzního inženýrství, digitální forenzní analýzou, apod.) tento incident, vydat doporučení pro ostatní subjekty KII, apod., aby se podobným incidentům do budoucna předcházelo, respektive aby byly příště lépe zvladatelné.

Poslední oblast s názvem „krizový management" je nezbytnou součástí ochrany KII. Zvládání a minimalizace dopadu jakéhokoliv narušení společnosti a státních struktur skrze kyberprostor musí být zakomponováno do celkového krizového managementu státu. Stát proto musí zahrnout ochranu KII do národních struktur krizového řízení. V závislosti na krizovém managementu každého státu se zakotvení ochrany KII opět liší. Nicméně platí, že gestor zodpovědný za ochranu KII má být situován tak, aby měl přístup k subjektům s rozhodovací pravomocí a v případě větší, celonárodní krize musí tento subjekt být i schopen spolupracovat a poskytovat poradenství přímo vládě. V rámci svých kompetencí by pak tento subjekt měl mít zákonně stanovenou gesci za celou oblast ochrany KII a měl by spolupracovat s různými partnery napříč státní i soukromou sférou.

## Závěr

Tento přehledový článek popsal v obecné rovině, jakým způsobem má stát působit v rámci zajišťování kybernetické bezpečnosti a v čem spočívá jeho role. Po teoretickém představení základních pojmů nutných pro účely tohoto článku se značná část textu věnovala čtyřem hlavním oblastem, v nichž má stát možnost navyšovat svou kybernetickou bezpečnost: činnost policejních složek (vymáhání práva); činnost zpravodajských služeb; činnost vojenských složek (kybernetická obrana), a ochrana KII. V každé z nich pak byla vždy vymezena působnost státu, představen výběr (nikoliv vyčerpávající) základních nástrojů a metod využívaných v dané oblasti a na jejich bázi byla také stručně definována problematická místa.





Jak je zřejmé z textu, narůstající propojení státu a společnosti jako celku s kyberprostorem a prostředky ICT mění neustále roli státu v rámci zajišťování kybernetické bezpečnosti a lze pozorovat posouvání hranice působnosti státu v kyberprostoru. Konkrétní působení a naplňování role státu jako garanta kybernetické bezpečnosti se však liší stát od státu. Avšak ať již bude stát působit v kyberprostoru jakkoliv, musí se vždy zaměřit na několik stěžejních bodů. Zejména se zde jedná o legálnost státních aktivit v kyberprostoru, při nichž se využívají metody, techniky a nástroje, které nemusí být vždy právně nezávadné a mohou neoprávněně zasahovat do práv a svobod druhých osob.

Výzvou pro všechny státy je zde i pochopit nutnost zajišťování kybernetické bezpečnosti, aniž by se snažily bojovat proti samotné architektuře kyberprostoru a podkopávaly jeho výhody. Státy by pak rozhodně neměly ignorovat svou roli nebo povinnosti vůči svým občanům a musí uznat a neustále reflektovat strukturální omezení jejich moci.

V neposlední řadě je také nutno zmínit, že role státu v kyberprostoru je neustále oslabována samotným charakterem kyberprostoru, který vůči tradičnímu fungování státu, potažmo vlády, působí mimo jiné i negativně. Zejména se jedná o oslabování role státu skrze velmi lehce dostupné anonymizační prostředky a nástroje a také problém teritoriality. V oblasti kybernetické bezpečnosti tak struktura internetu může působit proti státu a výrazně tak limitovat jeho tradiční sílu. Síla státu je totiž spjata s jeho územím, což znamená, že je nejúčinnější, když může působit na fyzickou stránku kyberprostoru na svém území. Sofistikovaní aktéři se tak mohou schovávat za jurisdikční nejednotnost internetu a stát má tedy opět ztíženu roli garanta kybernetické bezpečnosti.

## Literatura

BAGGILI, Ibrahim a BREITINGER, Frank. Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer. In: Sociotechnical Behavior Mining: From Data to Decisions? Papers from the 2015 AAAI Spring Symposium, 2015 [online]. [cit. 2015-06-10]. Dostupný z: http://www.aaai.org/ocs/index.php/SSS/SSS15/paper/viewFile/10227/10092.

BASSETT, Richard, BASS, Linda a O'BRIEN, Paul. Computer forensics: An essential ingredient for cyber security. In: *Journal of science and technology*. Vol. 3, No. 1, 2016. ISSN 1545-0287.

BAYUK, Jennifer L. (et al.). *Cyber security policy guidebook*. Hoboken: John Wiley, 2012. ISBN 978-1-118-02780-6.

BERKA, Petr. *Dobývání znalostí z databází*. Praha: Academia, 2003. ISBN 80-200-1062-9.

BRAVO, Rogerio. Open sources in cybercrime investigation: concept and implications, 2014 [online]. [cit. 2015-06-10]. Dostupný z: http://www.academia.edu/7301278/OPEN_SOURCES_IN_CYBERCRIME_INVESTIGATION_concept_and_implications.

Bezpečnostní strategie České republiky, 2015 [online]. [cit. 2015-06-10]. Dostupný z: http://www.mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_2015.pdf.

DEMAREST, Geoffrey B. Espionage in International Law. In: Denver Journal of International Law and Policy. Vol. 24, 1996. ISSN 0196-2035.

DETERMANN, Lothar a GUTTENBERG, Karl T. On War and Peace in Cyberspace. In Hastings constitutional law quarterly. Summer. Vol. 41, No. 4, 2014 [online]. [cit. 2015-06-10]. Dostupný z: http://www.hastingsconlawquarterly.org/archives/V41/I4/Determann_Online.pdf.

DUVENAGE, Petrus a SOLMS, Sebastian von. Putting Counterintelligence in Cyber Counterintelligence: Back to the Future, 2014. In: LIAROPOULOS, A. – TSIHRINTZIS (eds.). Proceedings of the 13th European Conference on Cyber Warfare and Security ECCWS-2014. Reading: Academic Conferences and Publishing International Limited. ISBN 978-1-910309-25-4.

EDWARDS, M. (ed.). Critical Infrastructure Protection. Amsterdam: IOS Press BV, 2014. ISBN 978-1-61499-356-8.

FRANK, Libor. Analýza a predikce bezpečnostních hrozeb a rizik v České republice. Disertační práce. Brno: FSS MU, 2006.

FRANK, Libor. Bezpečnostní politika. In: ZEMAN, Petr et al. Česká bezpečnostní terminologie: Výklad základních pojmů. Brno: Vojenská akademie v Brně, 2002 [online]. [cit. 2015-06-10]. Dostupný z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.

FRIEDMAN, Allan a SINGER, Peter W. Cybersecurity and cyberwar. What everyone needs to know. New York: Oxford University Press, 2014. ISBN 978-0-19-991811-9.

GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: CCD COE Publication, 2011. ISBN 978-9949-9040-5-1.

GUARDIAN. Booz Allen Hamilton: Edward Snowden's US contracting firm, 2013 [online]. [cit. 2015-06-10]. Dostupný z: http://www.theguardian.com/world/2013/jun/09/boozallen-hamilton-edward-snowden).

HARRIS, Shon. CISSP All-In-One Exam Guide. Columbus: McGraw-Hill, 2013. ISBN 978-0-07-178173-2.

HEALEY, Jason a WILSON, A. J. Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain, 2013 [online]. [cit. 2015-06-10]. Dostupný z: http://mercury.ethz.ch/serviceengine/Files/ISN/160116/ipublicationdocument_singledocument/2a41383f-8970-4c32-9193-845067598ece/en/bsc130221cyberwprpub.pdf

CHESTERMAN, S. The Spy Who Came in from the Cold War: Intelligence and International Law. In: Michigan Journal of International Law, Vol. 27, 2006. ISSN 1052-2867.

JIRÁSEK, Petr, NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie České republiky, 2015. ISBN 978-80-7251-436-6.

LIMNÉLL, Jarno. Controversial active cyber defense, 2012 [online]. [cit. 2015-06-10]. Dostupný z: http://www.infosecisland.com/blogview/22757-Controversial-Active-Cyber-Defense.html.





LIMNÉLL, Jarno. Offensive cyber capabilities are needed because of deterrence. In: RANTAPELKONEN, Jari a SALMINEN, Mirva. (eds.): The fog of cyber defence. Tampere: National defence university, 2013. ISBN 978-951-25-2430-3.

MAREŠ, Miroslav. Bezpečnost. In: ZEMAN, Petr et al. Česká bezpečnostní terminologie: Výklad základních pojmů. Brno: Vojenská akademie v Brně, 2002 [online]. [cit. 2015-06-10]. Dostupný z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.

MCGUFFIN, Chris. On domains: Cyber and the practice of warfare. In: International Journal: Canada's Journal of Global Policy Analysis, Vol. 69, No. 3, 2014. ISSN 0020-7020.

MORGENTHAU, Hans J. Politics among nations: the struggle for power and peace. New York: Knopf, 1948. bez ISBN.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, 2015. [online]. [cit. 2015-06-10]. Dostupný z: https://www.govcert.cz/download/nodeid-1004/.

PAČKA, Roman. Difference Between Cyber Security and Cyber Defence from a Czech Perspective. In: Cyber Security Review, Spring ed., London: Delta Business, 2015. ISSN 2055-6950.

PAPPALARDO, Joe. NSA Data Mining: How It Works, 2013. [online]. [cit. 2015-06-10]. Dostupný z: http://www.popularmechanics.com/military/a9465/nsa-data-mining-how-it-works-15910146/.

PURPURA, Philip. Security and Loss Prevention: An Introduction. San Diego: Butterworth-Heinemann, 2007. ISBN 978-0-08-055400-6.

RADSAN, John A. The Unresolved Equation of Espionage and International law. In: Michigan Journal of International Law, Vol. 28, No. 597, 2007. ISSN: 1052-2867.

ROSENZWEIG, Paul. The Evolution of Wiretapping. In: Criminal Law & Procedure. Volume 12, Issue 2, 2011 [online]. [cit. 2015-06-10]. Dostupný z: http://www.fed-soc.org/library/doclib/20110912_RosenzweigEngage12.2.pdf.

SCHNEIER, Bruce. *Data and Goliath*. New York: Norton, 2014. ISBN 978-0-393-24481-6.

SMOLÍK, Josef. *Úvod do studia mezinárodních vztahů*. Praha: Grada Publishing, 2014. ISBN 978-80-247-5131-3.

SOLOMON, Michael, BARRETT, Diane a BROOM, Neil. Computer Forensics Jump Start. San Francisco: Sybex, 2005. ISBN: 978-0-470-93166-0.

SUTER, Manuel. A generic national framework for critical information infrastructure protection (CIIP). Zurich: ITU, 2007 [online]. [cit. 2015-06-10]. Dostupný z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

SVFORUM. Security SIG: Guerilla anti-penetration tactics, 2003 [online]. [cit. 2015-06-10]. Dostupný z: https://svforum.org/Software-Architecture-and-Platform/Security-SIG-Guerilla-Anti-Penetration-Tactics.

WESTBY, Jody. Caution: Active response to cyber attacks has high risk, 2013 [online]. [cit. 2015-06-10]. Dostupný z: http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

Zákon č.181/2014, Sb, o kybernetické bezpečnosti a o změně souvisejících zákonů. In Sbírka zákonů. 29. srpna 2014. ISSN 1211-1244 [online]. [cit. 2015-06-10]. Dostupný z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6688.

**RESUMÉ**

Tento článek se zabývá vymezením role státu v oblasti zajišťování kybernetické bezpečnosti. Konkrétně si klade za cíl vymezit roli státu a vytvořit základní přehled o působení státu v kyberprostoru, které rozčleňuje celkem do čtyř oblastí: činnost policejních složek (vymáhání práva); činnost zpravodajských služeb; činnost vojenských složek (kybernetická obrana) a ochrana kritické informační infrastruktury. V každé z těchto oblastí se pak detailněji věnuje výčtu jednotlivých metod, nástrojů či technik, které stát v dané oblasti využívá. V neposlední řadě tento článek stručně představuje i základní problematické oblasti, kterým stát musí při zajišťování kybernetické bezpečnosti čelit.

**Klíčová slova:** kybernetická bezpečnost, kybernetická obrana, informační kriminalita, role státu, kybernetická bezpečnostní politika, zpravodajské služby, kritická informační infrastruktura.

**SUMMARY**

*PAČKA, Roman: THE STATE ROLE IN ENSURING CYBER SECURITY*

This article deals with defining the state role in ensuring cyber security. In particular, it aims to explain the role of the state and create the basic overview of the state activities in the cyberspace. These activities are divided into four areas: law enforcement, intelligence services´ activities, cyber defence and protection of critical information infrastructure. In each of these areas a detailed list of the various methods, tools and techniques is presented. Last but not least, this article identifies the fundamental problem areas that must be addressed by the state in order to ensure cyber security.

**Keywords:** cyber security, cyber defence, cyber-crime, state role, cyber security policy, intelligence services, critical information infrastructure.





*JUDr. Simona Diblíková*
*Institut pro kriminologii a sociální prevenci*

# Elektronický monitoring v Evropě[1]

## Úvod

Elektronický monitoring je zde chápán jako všeobecný termín vztahující se k různým formám sledování osoby v rámci trestního procesu; její polohy, pohybu a chování.[2] Je považován za humánní a důvěryhodnou alternativu k uvěznění, kdy napomáhá udržení sociálních vazeb pachatele a nenarušuje jeho ekonomickou situaci. Pokud jsou technologie elektronického sledování používány přiměřeně a podle stanovených pravidel, jsou redukovány negativní dopady na osobní a rodinný život monitorované osoby a ostatních zúčastněných (rizika tzv. net-widening efektu[3]). U elektronického monitorování se předpokládá zajištění efektivního dohledu nad pachateli ve společnosti, účinné kontroly výkonu uložených povinností a omezení, a přispění k prevenci kriminality.

V evropských zemích[4] je elektronické sledování pro účely trestní justice využíváno od devadesátých let minulého století. V současné době ho aktivně užívá více než 20 zemí a další (vč. České republiky či Slovenska) jsou v různých postupných fázích implementace. Zavádění a očekávané fungování elektronického sledování vyvolává velké naděje, je ale nutné zdůraznit, že se jedná pouze o nástroj výkonu opatření, jakkoli užitečný. Nicméně politické klima je pro zavádění elektronického monitoringu příznivé a nahrává tomu i fakt, že opět narůstají počty vězněných osob a používané technologie se vylepšují. V případě tvorby konceptu elektronického monitoringu hrají významnou roli média, která mohou mírnit nerealistická očekávání a naopak propagovat silné stránky a dobrou, ověřenou praxi.

Autorství teoretického konceptu elektronického sledování osob je připisováno psychologu Harvardské univerzity R. Kirklandu Schwitzgebelovi (příjmení později zkracováno na Gable) a jeho bratru Robertovi. Po experimentech se skupinou

[1] Širší materie byla autorkou a JUDr. Petrem Zemanem (Institut pro kriminologii a sociální prevenci) vytvářena pro potřeby pracovní skupiny Ministerstva spravedlnosti EMSON (Elektronický monitorovací systém „ON"), která měla primárně za cíl přípravu podkladů k zavedení elektronického monitoringu pro trestní justici v České republice. Medailonky jednotlivých evropských zemí jsou prezentovány na webu www.justice.cz

[2] Recommendation CM/Rec(2014)4 of the Committee of Ministers to Member States on Electronic Monitoring, Definitions, s. 2, Council of Europe, February 2014.

[3] Viz CM Documents CM(2014)14 add 2. Commentary to Recommendation of the Committee of Ministers to Member States on Electronic Monitoring, Rule 3, s. 3, Council of Europe, January 2014.
Srov. též ZÁHORA, J. Európské štandardy pre monitorovanie osob v trestnom konaní. *Trestněprávní revue*. 11-12/2014, s. 258 a pozn. pod čarou č. 18.

[4] Data byla čerpána z dotazníkových šetření v letech 2009, 2011, 2012 a 2013 (Survey of Electronic Monitoring in Europe: Analysis of Questionnaires), která k problematice využívání elektronického monitorovacího systému mezi zástupci svých členských zemí realizuje organizace CEP - Permanent European Conference on Probation and Aftercare (www.cep-probation.org)