New Direction

Miroslav Mareš

KYBERNETICKÁ BEZPEČNOST

Vybrané aktuální výzvy a problémy z pohledu České Republiky

newdirection.online @europeanreform @europeanreform NDeuropeanreform contact@europeanreform.org

New Direction

Founded by Margaret Thatcher in 2009 as the intellectual hub of European Conservativism, New Direction has established academic networks across Europe and research partnerships throughout the world.

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
REGISTERED OFFICE: Rue du Trône, 4, 1000 Brussels, Belgium. EXECUTIVE DIRECTOR: Naweed Khan.

Miroslav Mareš

Prof. JUDr. PhDr. Miroslav Mareš, Ph.D. (1974) vystudoval politologii a právo na Masarykově univerzitě v Brně. Odborně se zaměřuje na výzkum bezpečnostní politiky a bezpečnostních hrozeb (zvláště extremismu a terorismu) v prostoru střední a východní Evropy, včetně jejich kybernetické dimenze. Autor či spoluautor více než 300 odborných publikací.

Zdroj obrázků:
Printscreen hacknuté stránky s doménou .cz z roku 2022 a budova Národního úřadu pro kybernetickou a informační bezpečnost v Brně, foto M. Mareš 2021 ©

OBSAH

SHRNUTÍ HLAVNÍCH ZJIŠTĚNÍ A DOPORUČENÍ

– Česká republika disponuje na poli terminologie kybernetické bezpečnosti dostatečným zázemím, je však třeba objasňovat tuto problematiku osobám rozhodujícím v politice a odpovídajícím způsobem i širší veřejnosti (zvláště pokud se týká rozdílu mezi bezpečností a hrozbami v kyberprostoru celkově a kybernetickou bezpečností v užším pojetí);

– V ČR existuje robustní systém státních orgánů, specializovaných strategických, i koncepčních dokumentů a expertů zabývajících se kybernetickou bezpečností, je však třeba zajistit i dostatečný počet expertů na další rozvoj na daném poli (mj. v kontextu přejímání směrnice NIS2) a vhodně zařadit problematiku kybernetické bezpečnosti do širších strategických dokumentů v ČR;

– Kybernetickou bezpečnost by měl vhodně koordinovat Poradce pro národní bezpečnost tak, aby identifikoval slabá místa ve spolupráci a v případném nevhodném překrývání kompetencí některých orgánů a efektivně spolupůsobil při zapracování této problematiky do strategických dokumentů v bezpečnostní oblasti;

– Národní centrála proti terorismu, extremismu a kybernetické kriminalitě v rámci kybernetické bezpečnosti ČR by měla efektivně využívat vzájemnou spolupráci expertů z IT-sféry a expertů na terorismus a extremismus a flexibilně reagovat na nové trendy, včetně využití kriminálního zpravodajství pro odhalování kybernetické kriminality;

– Je třeba odborně vyjasnit a podpořit vyšetřování a stíhání kyberteroristické činnosti v kontextu § 311, § 312a a § 313 trestního zákoníku, především ve vztahu k aplikaci takové činnosti skupinou ve smyslu § 129a trestního zákoníku;

– Je třeba odborně vyjasnit a podpořit vyšetřování a stíhání trestné činnosti kybernetických bojovníků v cizích ozbrojených silách a nestátních ozbrojených skupinách ve smyslu § 321 a § 321a trestního zákoníku;

– Je třeba najít vhodné právní nástroje na postih nových forem anebo nové intenzity kybernetické kriminality, odpovídajícím způsobem prosadit zájmy ČR do komplexní mezinárodní úmluvy o boji proti využívání informačních a komunikačních technologií pro účely trestné činnosti, přičemž je třeba důsledně žádat i postih a efektivní spolupráci při vyšetřování přiřazení útoků kriminálním strukturám, které některý stát autorizuje k uskutečnění zločinu proti jinému státu či mezinárodní organizaci;

– Důsledně je třeba i nadále podporovat multioborovou dlouhodobě zaměřenou spolupráci státu, soukromé sféry a akademických pracovišť na poli aplikovaného i základního výzkumu a vzdělávání na poli kybernetické bezpečnosti a kybernetické obrany.

ÚVOD

Cílem této stude je představit vybrané aktuální výzvy a problémy, které jsou spojeny s kybernetickou bezpečností, a to primárně z hlediska bezpečnostní politiky České republiky. Studie je zaměřena na identifikaci takových výzev a problémů, které jsou důležité z hlediska soudobého a budoucího vývoje. Oborově studie spadá do „policy" analýz a je psána v rámci politologického přístupu a přístupu společensko-vědně zaměřených bezpečnostních studií. Neobsahuje tedy přístupy kybernetiky a vědy k informačním technologiím, pouze v dílčích aspektech referuje o poznatcích těchto disciplín. Snaží se upozornit na vybrané trendy a události v bezpečnostní oblasti, které je potřeba reflektovat a případně řešit na úrovni státní bezpečnostní politiky.

Nejedná se tedy o komplexní přehled kybernetické bezpečnosti v ČR, ale jde o mimořádně rozsáhlou multioborovou problematiku, u které lze navíc odkázat na již existující literaturu (Doucek, Konečný, Novák 2019, Pačka 2019). I když ve studii budou dílčím způsobem řešeny právní otázky, i v této oblasti jsou již podstatné problémy zpracovány (Polčák, Harašta, Stupka 2016), totéž lze konstatovat o rozborech kyberkriminality (Smejkal 2022, Završník 2017) a částečně i kybernetické obrany (Feix, Procházka 2017, Pačka, Mareš 2022).

Ve studii budou nejprve shrnuty hlavní koncepční výzvy, které se týkají problematiky kybernetické bezpečnosti v ČR, následovat bude analýza jejích silných a slabých stránek. Poté budou řešeny aktuální problémy, a to výzvy v oblasti koordinace kybernetické bezpečnosti pro nově vznikajícího národního poradce pro bezpečnost, role nové Národní centrály proti terorismu, extremismu a kybernetické kriminalitě v rámci kybernetické bezpečnosti ČR. Ve vazbě na ně pak problematika teroristického útoku spáchaného v kyberprostoru dle § 311 trestního zákoníku, otázky obecné a právní konceptualizace zahraničních „kyber-bojovníků" a vybraných forem extremistické a teroristické kriminality s vazbami na kybernetickou bezpečnost. Závěrem budou shrnuty poznatky a identifikovány prvky důležité pro politické rozhodování na daném poli i připomenutí aktuálních vývojových trendů na poli kybernetické bezpečnosti a obrany, včetně shrnujícího stanoviska pro potřebu multi-oborového výzkumu a vzdělávání v oblasti kybernetické bezpečnosti.

V celém textu je primárně používán termín kybernetická bezpečnost, což odpovídá terminologii užívané v českém právu i v hlavních koncepčních dokumentech. Přestože část expertů razí zkracující termín kyberbezpečnost, držím se zde uvedené právně-úřední terminologie.

1

ZÁKLADNÍ PROBLEMATIKA S VYMEZENÍM A POJETÍM KYBERNETICKÉ BEZPEČNOSTI V KONTEXTU BEZPEČNOSTNÍ POLITIKY A BEZPEČNOSTNÍHO SYSTÉMU ČR

Pokud se týká definice pojmu kybernetická bezpečnost, není explicitně uveden v domácích právních normách. Podle definice v normě Mezinárodní organizace pro standardizaci (ISO), kterou používají i čeští experti (Doucek, Konečný, Novák 19) se jedná o „zabezpečení (safeguarding) lidí, společnosti, organizací a národů před kybernetickými riziky“ (přičemž zabezpečením se myslí udržení kybernetických rizik na „tolerovatelné úrovni“) (IECISO/IEC TS 27100:2020, 2020). Expertní definice kybernetické bezpečnosti, používaná i v úřední sféře v ČR, je následující: „Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“ (Jirásek, Novák, Požár 2019: 69).

Obě tyto definice jsou však poměrně široké z hlediska toho, jak je kybernetická bezpečnost chápána v kontextu platného zákona č. 181/2014 o kybernetické bezpečnosti, v platném znění, z hlediska Národní strategie kybernetické bezpečnosti na léta 2021–2025 i různých norem EU a pojetí NATO. Bezpečnost v kybeprostoru je mnohem širší kategorií, než jaké je pojetí v uvedených dokumentech.

Kyberprostor je přitom ze strany NATO definován následovně: *„Globální doména tvořená všemi vzájemně propojenými komunikačními a informačními systémy a dalšími elektronickými systémy, sítěmi a jejich daty, včetně těch, které jsou oddělené nebo nezávislé, které zpracovávají, ukládají nebo přenášejí data.“* (North Atlantic Treaty Organisation 2022a: 100).

Velmi zjednodušeně lze konstatovat, že kybernetická bezpečnost je vztažena k zajištění bezpečnosti IT-zařízení a jejich digitálního obsahu celkově (hardware, software i datové soubory) před zásahem prostřednictvím kyberneticky vedeného útoku, a to ze sítě i z připojených zařízení. Oproti tomu bezpečnost v kyberprostoru se týká eliminace všech hrozeb, které se mohou vyskytnout v různých dimenzích virtuálního světa vytvářeného internetovými sítěmi. Jedná se tedy o hrozby týkající se například šíření dezinformací a propagandy, propagace terorismu a extremismu, šíření dětské pornografie, tzv. kyberšikanu pomocí diskreditujících videí, fotografií a textů, tzv. internetové podvody apod.

Kybernetická bezpečnost (v uvedeném úzkém smyslu) přitom může být propojena s fyzickou bezpečností, pokud dochází k využití kybernetických útoků pro způsobení škod ve fyzickém světě. Jedná se například o kybernetické útoky na nemocniční zařízení, na energetickou a dopravní infrastrukturu, na automatické řídicí systémy různých transportních prostředků, na přehradní nádrže apod.

„Tvrdá“ kyberbezpečnost může být specificky propojena s fyzickým světem, a to zvláště v kontextu

tzv. nepřátelských insiderů, tedy lidí, kteří mají přístup k IT-systémům (mj. k heslům) v soukromém i státním zařízení a za úplatu nebo z jiných důvodů je prozradí anebo je zneužijí k vlastním účelům. Kyberbezpečnost samozřejmě ovlivňují z jedné strany i schopnost, motivace a vybavení bránit se kybernetickým útokům a z druhé strany motivace, schopnosti a vybavení protivníka. Schopnosti i vybavení přitom nemusí být v případě některých typů útoků příliš sofistikované, například se to týká DDoS útoků. Pro hlavní oblasti hrozeb a pro obranu vůči nim v oblasti kybernetické bezpečnosti a kybernetické obrany jsou však samozřejmě vyžadovány vysoce kvalifikované znalosti, dovednosti a vybavení.

Obdobně jako pojem kybernetická bezpečnost, i pojem kybernetická kriminalita není vnímán zcela jednotně, nicméně v současné době lze konstatovat, že převládá jeho poměrně široké pojetí, vztažené k celkovému páchání kriminality v kyberprostoru, včetně obsahových aspektů. V zásadě se tedy vztahuje ke všem zločinům (respektive deliktům) v kyberprostoru. Autoři z kolektivu vedeného Tomášem Gřivnou a Radimem Polčákem definují kumulativně kyberzločin jako:

„a) trestný čin ohrožující ICT – informační a síťovou bezpečnost (trestný čin proti počítačové integritě nebo také trestný čin v úzkém pojetí);
b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům) a
c) trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat)“ (Gřivna, Polčák a kol. 2008: 35).

Jako specifický podtyp kybernetické kriminality s potenciálním přesahem do různých oblastí kybernetické bezpečnosti je možné vnímat i kyberterorismus, který v užším slova smyslu a velmi obecně znamená páchání teroristických útoků prostřednictvím počítačových systémů a sítí, nicméně někteří autoři pod tímto pojmem rozumí i vystavování teroristického obsahu (návody, propagace, „černé listiny“ nepřátel apod.) (Drmola 2013). Vhodnější je přitom spíše užší definice kyberterorismu, byť s vědomím toho, že tento typ útoků se zatím vyskytuje málo (chybí zde obvykle obecný definiční prvek terorismu, kterým je násilí) (Drmola 2013).

Kybernetická bezpečnost v širokém akademickém pojetí v sobě může obsahovat dimenzi vojenského i nevojenského vedení kybernetických útoků a operací. Pro pochopení soudobé situace v České republice, ale v zásadě i v rámci EU a NATO, je třeba mít na paměti, že kyberprostor se stal tzv. pátou doménou vedení bojové činnosti (vedle pozemního boje, námořního boje, vzdušného boje a kosmického boje) (Bastl, Gruberová 2013) a v daném kontextu byl uznán i ze strany NATO na Varšavském summitu v roce 2016. Kybernetická obrana (cyber defence) a kybernetická politika NATO jsou v rámci aliance systematicky rozvíjeny přinejmenším od pražského summitu v roce 2022 (Psychogiou 2022).

Z hlediska bezpečnostní politiky ČR je podstatné, že NATO používá pojem kybernetická obrana a tento pojem je užíván i v českém prostředí, včetně existence příslušných institucí a strategických a koncepčních dokumentů (viz níže). NATO definuje kybernetickou obranu jako *„Prostředky k dosažení a provedení defenzivních opatření s cílem čelit kybernetickým hrozbám a zmírnit jejich dopady, a tím uchovat a obnovit bezpečnost komunikačních, informačních nebo jiných elektronických systémů anebo informací, které jsou ukládány, zpracovávány nebo přenášeny v těchto systémech“* (North Atlantic Treaty Organisation 2022a: 99). NATO přitom počítá nejen s obranou, ale i s vedením ofenzivních kybernetických operací, které celkově vymezuje následovně: *„Činnosti prováděné v kyberprostoru nebo jeho prostřednictvím s úmyslem zachovat volnost jednání v kyberprostoru svou a vlastních a/nebo vytvořit účinky pro dosažení vojenských cílů“* (North Atlantic Treaty Organisation 2022a: 100).

V zásadě tedy lze v České republice identifikovat potřebu udržení kybernetické bezpečnosti v nevojenských situacích a potřebu kybernetické obrany a kybernetických ofenzivních operací ve vojenských situacích. I v nevojenských akcích je přitom třeba rozlišovat ochranu proti útokům a možnost zasáhnout protivníka (například vymazáním jeho dat, pokud např. provozuje stránky s návody na výrobu zbraní pro teroristy). Přestože intenzita a rozsah opatření v rámci kybernetické obrany může být výrazně vyšší než v případě „civilní“ kybernetické bezpečnosti, z čistě technického hlediska se jedná o obdobné činnosti. Proto je vymezení „kybernetické obrany“ dáno v zásadě účelem a aktérem, který ji provádí (tedy přináleží k vojenské oblasti).

Obdobně jako v řadě jiných oblastí je tedy i v případě kybernetické bezpečnosti třeba rozlišovat mezi akademickými koncepty a definicemi na straně jedné a úředními a právními definicemi na straně druhé. Je

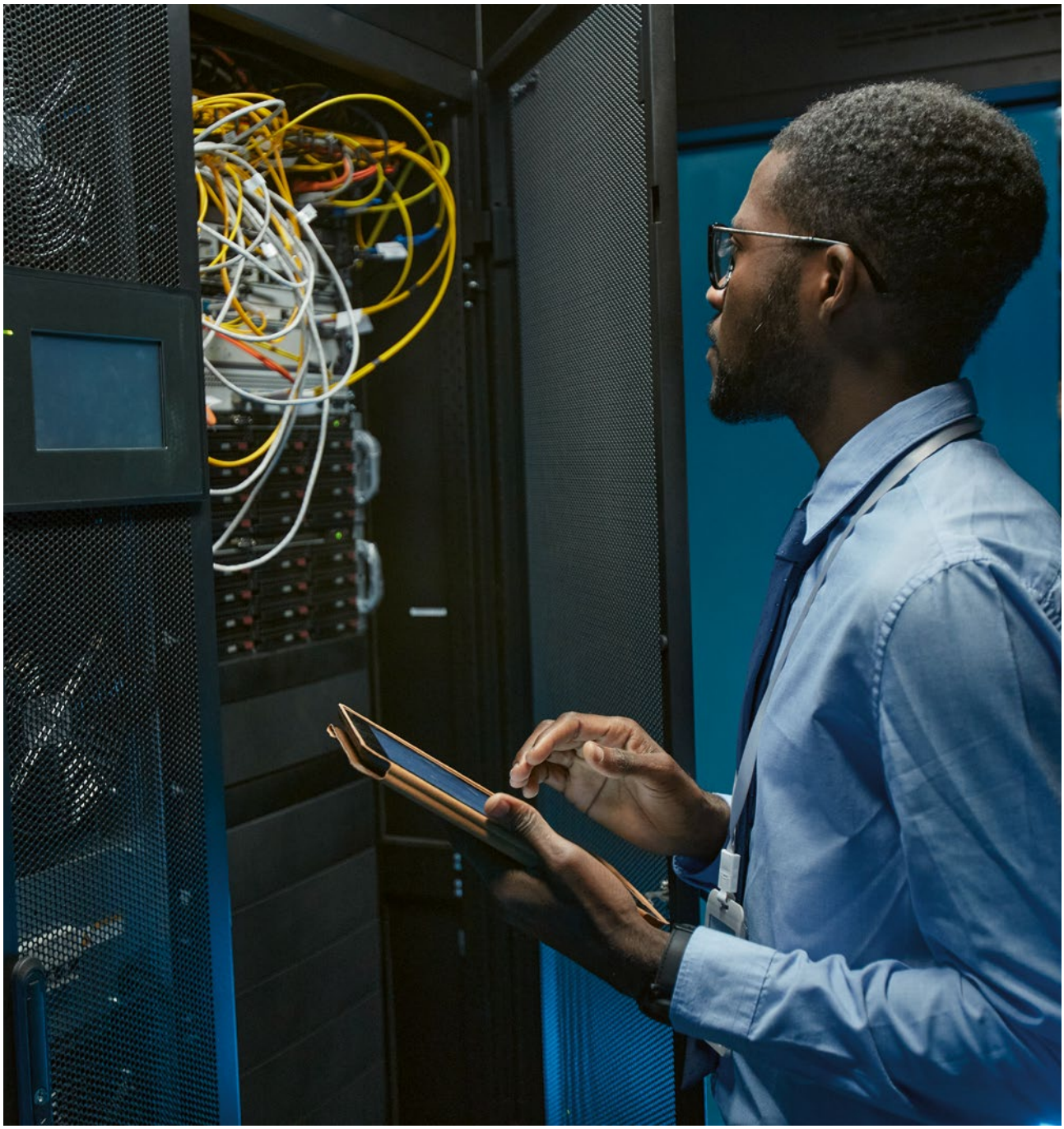
přitom třeba upozornit i na probíhající silnou evropeizaci politiky v oblasti kybernetické bezpečnosti, když postupně dochází ke sjednocování na evropské úrovni, a to za účasti členských států. I na úrovni EU přitom existuje rozdělení problematiky na obrannou (respektive vojenskou) část a na civilní kyber-bezpečnostní problematiku. O roli NATO v kybernetických operacích již byla zmínka výše. Dále je možné zdůraznit i výraznou roli, kterou se snaží hrát v roli proti kybernetické kriminalitě Rada Evropy (Csonka 2006).

Z hlediska bezpečnostní politiky ČR je tedy podstatné, že kybernetická bezpečnost je ovlivňována členstvím České republiky v mezinárodních organizacích, současně však ČR realizuje na tomto poli vlastní politiku a spolupodílí se na činnosti mezinárodních organizací s kyberbezpečnostním zaměřením. K tomu má Česká republika zpracovány i odpovídající bezpečnostní dokumenty (pozornost jim bude věnována v další kapitole) a instituce zabývající se kybernetickou bezpečností a kybernetickou obranou jsou součástí bezpečnostního systému České republiky.

V této souvislosti i s připomenutím předchozího nastínění debaty i vztahu akademických a úředních/právních konceptů je možné upozornit na skutečnost, že kybernetická bezpečnost v ČR i v mezinárodních organizacích, kterých je ČR členem, je vymezena ve specificky zaměřených částech bezpečnostních dokumentů, jsou na ni svým zaměřením a případně i názvem vázány státní instituce, soukromé společnosti a asociace i akademická výzkumná centra či odborná periodika a řady. Nicméně kyberbezpečnost prostupuje celým bezpečnostním systémem. V současné době lze v zásadě těžko najít státní instituci, která by nepotřebovala přinejmenším pasivní kybernetickou ochranu svých sítí a databází. I aktivní politika a činnost na poli kybernetické bezpečnosti je vlastní relativně širokému spektru aktérů. Tuto „celkovou průřezovost“ kybernetické bezpečnosti ve vztahu k bezpečnosti obecně je třeba mít na paměti při čtení dalších kapitol této knihy, kde samozřejmě s ohledem na rozsah a téma musí být pozornost zaměřena na hlavní specializované instituce a dokumenty.

Na druhou stranu je možné zmínit jinou skutečnost, která se projeví v analýze v některých kapitolách této studie, a tou je silná vazba (respektive závislost) kybernetické bezpečnosti na jiných sektorech bezpečnosti, specificky pak na energetické bezpečnosti. Masivní provoz počítačových sítí a techniky je podmíněn dostatkem elektrické energie. V případě dosavadního a současného dostatku elektrické energie je třeba rozpracovávat jiné formy ochrany, obrany i útočných operací než v případě masivního krátkodobého, a především pak střednědobého a dlouhodobého výpadku.

V nadcházejících kapitolách budou zpracovány především analýzy a predikce takových problémů na poli kybernetické bezpečnosti, které jsou aktuální vzhledem k připravovaným opatřením na státní úrovni v ČR anebo které představují specifickou výzvu s ohledem na bezpečnostně-politický vývoj i technologický vývoj na globální či regionální úrovni. Jako vhodný úvodní krok se proto jeví přehled silných a slabých stránek zajištění kybernetické bezpečnosti v ČR.



2

SILNÉ A SLABÉ STRÁNKY ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI V ČR

Česká republika má vybudovány v oblasti zajištění kybernetické bezpečnosti solidní základy, které jsou důsledkem dlouhodobého zájmu o danou problematiku ze strany širší expertní (epistemické) komunity i pochopení ze strany části politické reprezentace. Na straně druhé se pochopitelně i v této oblasti objevují určité deficity, které jsou dány jak nepochopením problematiky kybernetické bezpečnosti u některých osob rozhodujících v politice, tak i širšími problémy s limitovanými veřejnými zdroji, s demografickou situací i s dalšími okolnostmi.

Je přitom možné uvést, že vyhodnocení připravenosti ČR čelit kybernetickým hrozbám již bylo v minulosti několikrát uskutečněno, přinejmenším jednou pak i v širším bezpečnostním kontextu. Jednalo se o Audit národní bezpečnosti v roce 2016, kde byla jedna z kapitol věnována i hrozbám v kyberprostoru (jako tyto hrozby byly identifikovány dle důležitosti:

I) Kybernetická špionáž
II) Narušení nebo snížení odolnosti IT infrastruktury
III) Nepřátelské kampaně
IV) Narušení nebo snížení bezpečnosti eGovernmentu
V) Kyberterorismus) (Vláda ČR 2016: 95).

V dokumentu byla na prvním místě mezi silnými stránkami v rámci SWAT analýzy uvedeno: „Fungující, základní právně-legislativní rámec pro řešení kybernetické bezpečnosti“ (Vláda ČR 2016: 106).

Tuto silnou stránku je možné zdůraznit i v současnosti, respektive je možné k ní dodat i vhodnou strukturu strategických a koncepčních dokumentů v dané oblasti (až na jednu výjimku, viz níže), již relativně ustálenou institucionální strukturu zajištění kybernetické bezpečnosti a kybernetické obrany (k výjimkám viz následující kapitoly této studie) a navázané mezinárodní vztahy v dané oblasti. Ke slabším stránkám i nadále patří potřeba zajištění dostatečného množství expertů (což bylo konstatováno i v Auditu národní bezpečnosti) a v zásadě i občasná problematická politizace otázek kybernetické bezpečnosti (která následně vyvolává anebo ovlivňuje další problémy). Příkladem je nepochopení varování NÚKIB před produkty HUAWEI ze strany některých politiků a dalších relevantních aktérů v roce 2018 (Brokeš 2019).

V této kapitole nejdříve podrobněji nastíním pozitiva i dílčí problémy institucionální a následně právního a „strategicko-koncepčního“ základu. K detailům vybraných institucionálních výzev se pak vrátím ve specializovaných kapitolách. Pokud bych se měl na úvod pojednání vrátit k Auditu národní bezpečnosti, pak v daném kontextu je třeba upozornit na skutečnost, že v době jeho zpracování ještě tato problematika spadala výrazným způsobem do gesce Národního bezpečnostního úřadu. Teprve v roce 2017 (s účinností od 1. srpna) byl zřízen Národní úřad pro kybernetickou a informační bezpečnost, který je v současnosti ústředním orgánem státní správy (Zákon č. 205/2017 Sb.). Tento krok symbolizuje i prakticky dokazuje důležitost, kterou kybernetická bezpečnost v České republice získala, když se podařilo vytvořit zcela specializovaný úřad. Nicméně již v rámci Národního bezpečnostního úřadu byla kybernetické bezpečnosti věnována výrazná pozornost, což dokazuje existence Národního centra kybernetické bezpečnosti (NCKB) coby součásti NBÚ od roku 2012. Jeho tehdejší ředitel Vladimír Rohel v roce 2013 v rozhovoru pro časopis IT-System uvedl: *„Obecně prosazujeme myšlenku individuální odpovědnosti. Pokud tedy budeme například chtít po úřadech, aby prováděly analýzu bezpečnostních rizik, nebudeme určovat, jaké řešení a od kterého výrobce*

mají nasadit. Každý subjekt to musí vyhodnotit sám vzhledem ke svému systému" (Dolníček 2013). Nejen na základě tohoto konstatování lze odvodit, že kybernetická bezpečnost v ČR je zajišťována a plánována v multi-úrovňovém kontextu.

Pod NCKB byl při jeho vzniku zařazen i vládní CSIRT tým (Computer Security Incident Response Team). Jak vyplývá z analýzy předního českého experta na kyberbezpečnost Romana Pačky, činnost těchto týmů představovala ještě v hlubší minulosti české kyberbezpečnosti problematický prvek, protože mu nebyla věnována dostatečná pozornost ze strany státu ani soukromých firem. Jak Pačka píše, i *„když internet začal fungovat v ČR již v roce 1993, budování pracovišť typu CSIRT v ČR patřilo mezi dlouhodobě neplněné úkoly informační, respektive kybernetické bezpečnosti ČR"* (Pačka 2019: 48). Od roku 2001 však i na tomto poli začalo docházet ke zlepšování situace a v současné době má ČR k dispozici Vládní CERT (GovCERT.CZ) a týmy typu CSIRT plnící odpovědně zákonné povinnosti. Národní CERT zajišťuje organizace CZ.NIC (Národní úřad pro kybernetickou a informační bezpečnost 2022).

Paralelně k civilní struktuře kybernetické bezpečnosti se vyvíjely i vojenské struktury kybernetické obrany, tedy především Národní centrum kybernetických sil (NCKS), které vzniklo v rámci Vojenského zpravodajství v roce 2016 a poté bylo v roce 2018 přejmenováno na Národní centrum kybernetických operací (NCKO), přičemž právní specifikaci činnosti získalo v roce 2021 (Prucková 2021), a Velitelství kybernetických sil a operací (VeKySIOú), které v rámci Armády České republiky vzniklo v roce 2019 a v jehož rámci od roku 2020 působí Skupina kybernetických sil a operací (Havlík 2020) (jim se rovněž ještě dílčím způsobem budu věnovat v další kapitole).

Pokud se nyní vrátím k „civilní" kybernetické bezpečnosti, je třeba zmínit pionýrskou roli České republiky v přijetí zákona o kybernetické bezpečnosti, který se následně stal i jistým vzorem pro další státy světa. Byl přijat jako zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a od té doby byl několikrát novelizován, nicméně si zachovává své hlavní rysy, strukturu a jisté „právní poselství" pro charakter konceptualizace a zajištění kybernetické bezpečnosti v ČR. V přijetí zákona se výrazně angažoval tehdejší ředitel Národního bezpečnostního úřadu (a později první ředitel NÚKIB) Dušan Navrátil, který dokázal na této instituci vybudovat i silné multidisciplinární zázemí pro další rozvoj. Úzce spolupracoval i s akademickou sférou, přičemž v přípravě uvedeného zákona je třeba vyzdvihnout roli Radima Polčáka, vedoucího Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně.

Ještě před přijetím zákona se objevily v souvislosti se vznikem NCKB i precizní základy strategicko-koncepčního zajištění kybernetické bezpečnosti, a sice díky přijetí vládní Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012–2015. Na ni navázala Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 a v současnosti je platná Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025, ke které je přijat i příslušný akční plán (Národní úřad pro kybernetickou a informační bezpečnost 2022). V oblasti kybernetické obrany byla v roce 2018 představena Strategie kybernetické obrany na roky 2018–2022 (Riethofová 2018). V roce 2021 byl přijat novelizující zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony. V něm byly specifikovány úkoly a oprávnění VZ na poli kybernetické obrany.

Je tedy důležité, že ČR má k dispozici pro kybernetickou bezpečnost i kybernetickou obranu specializované strategie, které se snaží být vzájemně komplementární. U národních specializovaných strategií je třeba sledovat i soulad s národními strategiemi na vyšších i nižších úrovních i s dalšími specializovanými strategiemi (v ČR konkrétně na „kyberstrategii" odkazuje Národní strategie pro čelení hybridnímu působení (Ministerstvo obrany 2021) a současně soulad s obdobně zaměřenými dokumenty na evropské a mezinárodní úrovni, tedy především v rámci EU a v NATO. Evropská unie v roce 2020 přijala Strategii kybernetické bezpečnosti EU pro digitální dekádu, která celkově posiluje resilienci EU v této oblasti. Je v souladu s obdobnou národní strategií v ČR, u evropské strategie je charakteristický důraz na ochranu kyberprostoru v souvislosti se zaváděním 5G sítí (European Union 2020b). Strategie kybernetické bezpečnosti EU odkazuje na širší Strategii bezpečnostní unie EU, která je v zásadě strategií vnitřní bezpečnosti EU. V jejím rámci je kyberbezpečnosti a kybernetické kriminalitě rovněž věnována značná pozornost a poskytuje dobrý základ pro spolupráci členských zemí s EU v rámci této problematiky (European Union 2020).

Nicméně Česká republika nemá odpovídající strategii vnitřní bezpečnosti, která by na multiresortní bázi integrovala odolnost proti specifickým hrozbám, včetně odolnosti proti neválečným a nevojenským hrozbám v kyberprostoru. Má sice hlavní celkovou Bezpečnostní strategii České republiky, kde však s ohledem na její komplexní zaměření již zmiňovaný průřezový charakter kybernetické bezpečnosti není možné podrobněji zapracovat. O strategii vnitřní bezpečnosti již bylo několikrát v ČR uvažováno, doposud však nebyla schválena. Je přitom třeba zdůraznit, že její zpracování by bylo obtížné, protože by musela propojit přístupy více ministerských resortů (vnitra, spravedlnosti, práce a sociálních věcí, možná i částečně obrany apod.) i ústředních orgánů státní správy. Logicky by ji však koordinovalo ministerstvo vnitra, oblast kybernetické bezpečnosti by ale byla z velké části připravena ze strany NÚKIB.

Jednodušší je zapracování problematiky kybernetické obrany do Obranné strategie ČR, která má dominantně resortní charakter v rámci ministerstva obrany. V zatím poslední verzi z roku 2017 se po předchozím upozornění na hrozby v kyberprostoru nicméně pouze stručně konstatuje: *„Česká republika sama i ve spolupráci se spojenci aktivně rozvíjí své schopnosti v oblasti kybernetické bezpečnosti a obrany“* (Ministerstvo obrany České republiky 2017: 13). Mnohem větší pozornost je kybernetickým hrozbám a boji proti nim věnována v aktuální Strategické koncepci NATO, kde jsou přímo jako aktéři kybernetických hrozeb zmiňovány Rusko a Čína (North Atlantic Treaty Organisation 2022).

Z hlediska evropských závazků v oblasti kybernetické bezpečnosti je nyní aktuální a v zásadě hlavní výzvou implementace směrnice NIS2, která oproti dosavadnímu stavu klade důraz hlavně na malé operátory a odpovídající dohled nad nimi (v ČR jej realizuje NÚKIB). Pro zajištění směrnice je třeba dostatečný počet expertů na kyberbezpečnost, kterých je v ČR stabilně nedostatek. Proto je žádoucí podporovat studium stávajících studijních programů a stimulovat otevírání nových. Dosažení odpovídající kvalifikace vyžaduje i širší než pouze technické ICT znalosti. Určité možnosti k doplnění expertů, zvláště u soukromých firem, existují díky pracovní migraci.

Momentálně je vysoce kontroverzní otázkou zaměstnání profesně kvalifikovaných, ale bezpečnostně rizikových expertů, kteří uprchli z Ruska. Na jednu stranu je snad možné, že by pracovali v malých firmách, které nebudou mít strategický či taktický význam, nicméně i tak by mohli být „spícími agenty“ čekajícími na příležitost. Dosavadní tolerance Putinova režimu z jejich strany neposkytuje příliš silnou záruku jejich morální integrity. Zcela zapovězen by měl být každopádně přístup do strategicky významných soukromých firem (tento význam posilují i citlivé údaje o zaměstnancích) a do všech státních (v širokém pojetí) institucí. O specifickém využití pro „kyberpartyzánskou činnost“ bude pojednáno v jiné kapitole.

Pokud tedy má být shrnuto hlavní poselství této kapitoly, pak je jím to, že existující převážně kvalitní zákonné a strategické předpoklady je třeba naplnit, k čemuž přispívá věcný přístup těch, co v politice rozhodují. Důležité je zajistit odpovídající počet expertů na všech úrovních, k čemuž připívá atraktivita a využitelnost vzdělání v oboru. Do státní správy je však třeba vnést výrazné stimulace, aby experti nepreferovali pouze soukromý sektor. K tomu může přispět i „šíření entuziasmu“, který je na poli kybernetické bezpečnosti a obrany pracovní kultuře důležitých státních institucí vlastní. Rozvíjející se epistemická komunita expertů na kyberbezpečnost na národní a na vybrané lokální úrovni (typicky v tzv. brněnském Silicon Valley s vazbami do státních úřadů činných v kybernetické bezpečnosti a obraně) je rovněž příslibem budoucího pozitivního vývoje. Celou oblast kybernetické bezpečnosti a kybernetické obrany je třeba i odpovídajícím způsobem koordinovat na vládní úrovni.

3

KOORDINACE KYBERNETICKÉ BEZPEČNOSTI V ČR – ÚKOL PRO PORADCE PRO NÁRODNÍ BEZPEČNOST?

Ve vládním prohlášení z ledna 2022 bylo v části „Vnitřní bezpečnost a veřejná správa“ uvedeno: Do konce roku 2022 zřídíme při Úřadu vlády ČR pozici *„Poradce pro národní bezpečnost jako nadresortního koordinátora hybridních hrozeb, dezinformací a dalších závažných nadresortních bezpečnostních problematik. Na Úřadu vlády tak vznikne platforma pro koordinaci a komunikaci mezi subjekty bezpečnostní politiky s cílem zajistit užší spolupráci zpravodajských a bezpečnostních složek a efektivní postup proti dezinformacím a hybridním hrozbám“* (Vláda České republiky 2022).

V této souvislosti je možné a potřebné se zamýšlet i nad tím, jakou roli má mít tento „Poradce pro národní bezpečnost“ v koordinaci politiky v oblasti kybernetické bezpečnosti (a případně kybernetické obrany). Stávající Národní strategie kybernetické bezpečnosti ČR na období let 2021–2025, ani akční plán k ní s tímto poradcem nepočítají. Nicméně tato strategie vychází z hlavní řídicí role vlády (viz níže) a Národní poradce pro bezpečnost bude vládním úředníkem (Úřad vlády je nicméně ústředním orgánem státní správy ve smyslu kompetenčního zákona č. 2/1969 Sb.).

Na jednu stranu je zřejmé, že na poli kybernetické bezpečnosti je aktivních vícero institucí a tato problematika zasahuje do několika sfér, na straně druhé je třeba zmínit i již zákonem i jistými zvyklostmi vymezené role jednotlivých institucí a dalších aktérů, ve kterých nový aktér může začít působit za určitých okolností kontroverzně. Neměl by tudíž zasahovat do již stanovených a osvědčených kompetencí jiných a současně by neměl koordinovat chybně.

V souvislosti s již vytvořenými strukturami je třeba nicméně upozornit na již vícekrát zdůrazněné skutečnosti, že kybernetická bezpečnost je úzce prolnuta s dalšími sektory bezpečnosti a současně se dotýká množství vládních, soukromých komerčních, nevládních neziskových i akademických subjektů. ČR je navíc propojena s mezinárodním prostředím a jednotlivé české státní složky aktivní na poli kybernetické bezpečnosti a obrany mají svoje zákonně a úředně stanovené role, včetně propojení na příslušné zahraniční, supranacionální i mezinárodní struktury. Česká republika navíc zabezpečuje kybernetickou ochranu specifických mezinárodních institucí a organizací, které se nacházejí na jejím území (specificky pak Agentury Evropské unie pro kosmický program se sídlem v Praze). Mezinárodní rozměr má i kybernetická ochrana velkých soukromých komerčních subjektů, které uskutečňují vlastní ochranu na transnacionální korporátní úrovni (musí však pochopitelně dostát i závazkům vyplývajícím z práva ČR).

Role poradce pro národní bezpečnost tedy musí spočívat v oblasti kybernetické bezpečnosti především ve třech základních dimenzích:

1) v koordinaci vládní politiky, která se kybernetickou bezpečností zabývá, na úrovni identifikace a případné nápravy institucionálních nedostatků, zvláště pak nevhodného překrývání kompetencí jednotlivých institucí anebo nenaplňování jejich plánované role v bezpečnostním systému v kontextu komplexního zajištění bezpečnosti ČR. Zjištění z této činnosti by se měla ve středně- a dlouhodobé perspektivě odrazit i v úpravě právních norem a v úpravě strategických a koncepčních dokumentů;

2) ve vyhodnocování souhrnných strategických i důležitých specifických aktuálních informací o dění v kybernetické bezpečnosti, předaných od jednotlivých institucí národnímu poradci a zakomponování odpovídajících zjištění do sektorově šířeji zaměřených bezpečnostních podkladů pro vládu, s případnými návrhy vládě na vhodná rozhodnutí a pokyny podřízeným institucím v aktuální bezpečnostní situaci;

3) ve vlastní analytické činnosti zaměřené na specifické aktuální problematiky (zpravidla ve smyslu zakomponování aktuálních výzev kybernetické bezpečnosti do širšího spektra aktuálních hrozeb a úsilí o jejich eliminaci), přičemž zpracované podkladové materiály budou sloužit i dalším složkám bezpečnostního systému ČR (včetně těch činných na poli kybernetické bezpečnosti), případně i vybraným zahraničním partnerům.

Nyní budou vybrané problémy z jednotlivých výše zmíněných bodů rozebrány podrobněji. Pokud se týká koordinace politiky, je skutečně třeba u poradce pro národní bezpečnost klást důraz na vyšší politickou úroveň, tedy nikoliv na snahu o „velení“ různým institucím, které se v rámci bezpečnostního systému ČR do ochrany a obrany před kybernetickými útoky zapojují. Nicméně poradce pro národní bezpečnost může hrát důležitou roli při slaďování kompetencí těchto institucí v právních normách (tedy v ústavních, zákonných i podzákonných normách i v rámci evropských a mezinárodních závazků ČR), ve strategických a koncepčních dokumentech (k tomu blíže viz další odstavec) i více či méně formalizovaných aspektech realizace bezpečnostní politiky. Národní poradce pro bezpečnost by se mohl v připomínkovém řízení vyjadřovat i k návrhům zákonů v bezpečnostní oblasti a měl by mít i odpovídající vazby na Legislativní radu vlády. Dlouhodobý monitoring, analýza, syntéza a identifikace problémových kompetenčních sporů nebo nepokrytých míst by měly být zakomponovány do celkového zlepšování bezpečnostního systému.

Důležité je samozřejmě to, aby Národní poradce pro bezpečnost měl jasně vymezené kompetence ve vztahu ke stávající Bezpečnostní radě státu (podle nepotvrzených informací v době psaní tohoto textu by měl být jejím tajemníkem), v oblasti kybernetické bezpečnosti pak ve vztahu k Výboru pro kybernetickou bezpečnost, který je jejím stálým pracovním orgánem. Výbor již má ve svém statutu vymezenu působnost v koordinaci plánování opatření k zajišťování kybernetické bezpečnosti ČR, konkrétně pak zejména:

a) zabezpečuje meziresortní spolupráci, projednává záměry plánovacích a koncepčních materiálů z oblasti kybernetické bezpečnosti, předkládaných ministerstvy a jinými ústředními správními úřady, a doporučuje jejich projednání v Bezpečnostní radě státu,
b) zabezpečuje meziresortní koordinaci plánovacích a přípravných aktivit v oblasti zajišťování kybernetické bezpečnosti, důležitých pro stabilitu a bezpečnost České republiky s důrazem na ochranu kritické informační infrastruktury,
c) posuzuje a projednává požadavky státních orgánů uplatňované v rámci zajišťování kybernetické bezpečnosti,
d) posuzuje a projednává dokumenty na základě usnesení Bezpečnostní rady státu,
e) zpracovává a projednává vlastní materiály,
f) projednává vyhodnocení meziresortních připomínkových řízení k materiálům vztahujícím se k působnosti Výboru a doporučuje jejich projednání v Bezpečnostní radě státu,
g) posuzuje, projednává a koordinuje základní zaměření činnosti zástupců České republiky v orgánech EU, NATO a dalších mezinárodních organizacích, navazuje, rozvíjí spolupráci s mezinárodními subjekty a přispívá k formování jednotného postoje v oblasti kybernetické bezpečnosti České republiky směrem do zahraničí (Vláda České republiky 2021).

Národní poradce pro bezpečnost bude mít oproti výboru charakter „každodenní“ pracovní činnosti, nikoliv tedy setkávání (byť častých) expertních zástupců. Oproti výboru by měl klást důraz na zprostředkování zjištěných problémů vládě a na koordinaci kybernetické bezpečnosti s dalšími bezpečnostními politikami. To se týká již ve vládním prohlášení explicitně zmíněných hybridních hrozeb, s ohledem na aktuální vývoj by však měl být kompetentní i v koordinaci reakcí na různé formy válečného ohrožení ČR (byť je ve vládním prohlášení řazen do kapitoly o vnitřní bezpečnosti).

Jak bylo uvedeno, problematika kybernetické bezpečnosti a kybernetické obrany by měla být vhodně a komplementárně zakomponována i do strategických a koncepčních dokumentů ČR. V tomto směru lze konstatovat precizní zpracování dokumentů v kompetenci NÚKIB i v kompetenci složek Ministerstva obrany. Z hlediska koordinační role národního poradce pro bezpečnost by měl být kladen důraz na integrální propojení těchto dokumentů s hlavní Bezpečnostní strategií ČR i s dalšími dokumenty, zaměřenými dominantně na jiné problematiky, které jsou s kybernetickou bezpečností propojeny.

V tomto směru by měl mít analytický aparát národního poradce pro bezpečnost důkladný přehled o aktuálních strategiích s dosahem (byť dílčím) do bezpečnostní oblasti v ČR i v mezinárodním prostředí a měl by v daném smyslu být nápomocen při tvorbě resortních i sub-resortních strategií. V této souvislosti by mohl rozvíjet a precizovat i vlastní databázi, která by se zaměřila na bezpečnostně orientované strategie. Specifická spolupráce by měla být navázána s Ministerstvem pro místní rozvoj, které v současnosti provozuje databázi všech strategických dokumentů ČR (Ministerstvo pro místní rozvoj 2022).

Jak uvádí Ministerstvo pro místní rozvoj, databáze strategií jako technický nástroj a na ni vázaná metodika přípravy veřejných strategií jako metodický nástroj *pomáhají postupně řešit následující problémy jako např.:*

– *dlouhodobě velmi rozdílné pojetí strategií;*
– *velké množství strategických dokumentů;*
– *různorodou úroveň zpracování strategických dokumentů;*
– *různou úroveň realizace strategických dokumentů;*
– *odlišnou strukturu strategických dokumentů;*
– *rozdílné časování strategických dokumentů;*
– *hodnocení naplňování strategických dokumentů a jejich aktualizace* (Ministerstvo pro místní rozvoj 2019: 4).

Nicméně Databáze strategií a s ní spojená institucionální struktura (především meziresortní Expertní skupina pro strategickou práci – ESSP) nemá z logiky věci za úkol řešit konkrétní věcné obsahové aspekty dokumentů. V tom by však mohl a měl sehrát důležitou roli v bezpečnostní oblasti (a tedy i kyberbezpečnostní oblasti) právě Národní poradce pro bezpečnost, jehož aparát by samozřejmě měl být v ESSP zastoupen, faktická forma jím realizované politiky by však na této skupině měla být nezávislá.

Pokud se týká uvedené koordinace činností různých institucí v oblasti kybernetické bezpečnosti, je na straně jedné třeba brát do úvahy důležitou a zákonem vymezenou roli NÚKIB coby ústředního orgánu státní správy, na straně druhé však mít na paměti i to, že NÚKIB není výkonnou složkou ve smyslu prvního odstavce článku 3 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky. V zákoně jsou v tomto odstavci přímo jmenovány ozbrojené síly (v jejich rámci tedy i AČR a VKYSiO), ozbrojené bezpečnostní sbory (a v jejich rámci tedy i Policie ČR a její složky zabývající se kyberkriminalitou), záchranné sbory a havarijní služby (Mareš, Novák 2019: 129). V širším pojetí lze pod ozbrojené bezpečnostní sbory řadit i zpravodajské služby (Mareš Novák 2019: 133), byť o takovém pojetí lze diskutovat.

Nicméně obecně ani v sektoru kybernetické bezpečnosti NÚKIB není „nadřízeným“ orgánem bezpečnostních sborů, zpravodajských služeb a ozbrojených sil, byť s nimi samozřejmě na základě § 22 písm. g) zákona o kybernetické bezpečnosti spolupracuje a podle písmene e) v témže paragrafu má stanovenou koordinační roli orgánu ve stavu kybernetického nebezpečí (Zákon č. 181/2014 Sb.). Je třeba mít na paměti, že podle stávající verze Bezpečnostní strategie ČR za „zajišťování bezpečnosti státu a za řízení a funkčnost celého bezpečnostního systému ČR je odpovědná vláda jako vrcholný orgán výkonné moci“ (Vláda České republiky 2015: 23). Tato vládní role je uvedena i z hlediska systému kybernetické bezpečnosti v Národní strategii kybernetické bezpečnosti na období let 2021–2025 (Národní úřad pro kybernetickou a informační bezpečnost 2021: 8).

Za jiných okolností by však koordinační činnost měly vykonávat jiné orgány a vedle stávajícího výboru pro kybernetickou bezpečnost a Bezpečnostní rady státu je pro zařazení do širšího spektra problematik důležitá i jasně vymezená nová instituce, tedy Národní poradce pro bezpečnost. Důležité je, že na rozdíl od kolektivního rozhodování koordinačních výborů Bezpečnostní rady státu bude vládou jmenovaný poradce s vlastním aparátem akceschopnější.

Jeho přímý přístup k předsedovi vlády bude mít fakticky silný dopad na efektivitu přijatých rozhodnutí. Při vědomí této skutečnosti je však s ohledem na celkovou potřebu kontinuálně korektních vztahů v rámci bezpečnostního systému ČR zdůrazňovat „nevelitelskou“ roli národního poradce pro bezpečnost s tím, že formalizované a především neformalizované vztahy

s partnery ve všech sektorech bezpečnosti (nejen kybernetické bezpečnosti) se budou vyvíjet a stabilizovat postupně a budou odviset i od věrohodnosti osobnosti, která bude poradcem pro národní bezpečnost jmenována.

Již s ohledem na současnou situaci se jeví jako potřebné nejen jasně vymezit vztah a vazby mezi civilními institucemi v oblasti kybernetické bezpečnosti a vojenskými složkami v oblasti kybernetické obrany ve vztahu k aktuálním a budoucím hrozbám, ale i testovat efektivitu daného rozdělení modelováním a součinnostními cvičeními v různých bezpečnostních situacích za běžného bezpečnostního stavu a následně i za různých mimořádných bezpečnostních stavů, respektive i za fakticky válečné situace, za které nebude moct být válečný stav přepokládanou ústavní cestou vyhlášen (Mareš, Novák 2019: 56–58).

Národní poradce pro bezpečnost by obecně měl mít k dispozici aparát, který bude schopen připravovat kvalitní výstupy. Musí být komplexního náhledu na bezpečnost České republiky a v této souvislosti se jeví jako vhodné, aby do jeho kompetence přešla i příprava novelizací Bezpečnostní strategie ČR coby hlavního bezpečnostního strategického dokumentu. Je vhodné i jeho zapojení do mezinárodní spolupráce obdobných koordinátorů ze zahraničí a na evropské úrovni (Council of the EU 2022). V neposlední řadě se jeví jako potřebná jeho formalizovaná i neformalizovaná spolupráce s akademickou sférou, protože kontakty s výzkumníky i studenty mohou přinést důležité poznatky a impulsy pro činnost národního poradce pro bezpečnost, včetně oblasti kybernetické bezpečnosti.

4

ROLE NÁRODNÍ CENTRÁLY PROTI TERORISMU, EXTREMISMU A KYBERNETICKÉ KRIMINALITĚ V RÁMCI KYBERNETICKÉ BEZPEČNOSTI ČR

Na poli kybernetické bezpečnosti se od 1. ledna 2023 objeví nová instituce v rámci Policie České republiky, a sice Národní centrála proti terorismu, extremismu a kybernetické kriminalitě (NCTEK), která bude působit jako útvar s celorepublikovou působností v rámci Služby kriminální policie a vyšetřování Policejního prezidia Policie České republiky. Zřízení NCTEK odsouhlasil ministr vnitra a v době psaní tohoto textu již byl jmenován prvním ředitelem tohoto útvaru Břetislav Brejcha. Personální stav by měl být kolem 150 osob (Vaca 2022).

V době psaní tohoto textu nemám k dispozici bližší informace o struktuře NCTEK ani o vymezení jejích kompetencí ve vztahu k dalším policejním složkám, případně k jiným složkám bezpečnostního a justičního (v širším pojetí) systému. Nicméně s ohledem na stávající bezpečnostní vývoj a diskuse kolem vzniku a zaměření útvaru se pokusím analyzovat vybrané výzvy, které jsou se zřízením a přepokládanou činností NCTEK spjaty na poli kybernetické bezpečnosti.

Jak vyplývá z názvu, dominantně bude zaměřen na potírání třech forem kriminality, a sice extremismu, terorismu a kybernetické kriminality. Jedná se přitom o problematiky, které doposud byly řešeny na celostátní úrovni Národní centrálou proti organizovanému zločinu (NCOZ). Je přitom jasné, že zatímco extremismus a terorismus spolu úzce souvisí, kybernetická kriminalita představuje odlišný typ kriminality, respektive je to typ kriminality, který se prolíná s celou řadou dalších forem kriminality (nejen s extremismem a terorismem) a má i své svébytné formy.

NCTEK bude mít celostátní působnost, nicméně vůči krajským a okresním strukturám policie bude vykonávat pouze koordinační a metodickou činnost (Vaca 2022). Zatím není jasné, kolik bude mít nová centrála regionálních expozitur. Soudobé vedení ministerstva vnitra a velení Policie ČR se tedy rozhodlo jít cestou vzniku nového odštěpeného útvaru, což z hlediska policejní struktury signalizuje příklon k většímu počtu menších celostátních útvarů s vlastním zázemím. Je to v kontrastu např. s dřívější tzv. Langerovou reformou z druhé poloviny první dekády 21. století, která směřovala opačným směrem, tedy ke vzniku velkého centralizovaného Národního kriminálního úřadu (Mareš, Suchánek 2015: 84), který nakonec zřízen nebyl. Je přitom třeba zdůraznit, že NCTEK nevzniká zcela „na zelené louce“, ale navazuje na dlouhodobé řešení všech tří problematik v rámci jiných organizačních složek policie (respektive různě nazvaných předchůdců), naposledy tedy NCOZ. Lze předpokládat alespoň dílčí personální kontinuitu mezi NCTEK a NCOZ, byť přechod personálu je provázen i dílčími komplikacemi (Vaca 2022).

V rámci NCOZ existovala jednak sekce terorismu a extremismu (v jejím rámci mimo jiné působil

i Národní kontaktní bod pro terorismus) a jednak sekce kybernetické kriminality. Po linii kybernetické kriminality byla působnost NCOZ dána následovně: *„Trestné činy páchané formou kybernetických útoků vedených zejména vůči kritické a informační infrastruktuře včetně koordinace kybernetické kriminality, řešené nižšími organizačními celky v rámci struktury Policie ČR“* (Národní centrála proti organizovanému zločinu 2022: 7).

Již v úvodní kapitole byla kybernetická kriminalita vymezena z akademického pohledu, na tomto místě je možné upozornit na definici v pokynu policejního prezidenta č. 103/2013 ze dne 28. května 2013 o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení. V něm je kybernetická kriminalita chápana v relativně úzkém pojetí (ve vztahu k rozsahu akademických definicí), a to následovně. Kybernetickou kriminalitou je *„kriminalita, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kdy hlavním objektem útoku je samotná oblast informačních a komunikačních technologií a v nich obsažená data“* (Pokyn policejního prezidenta č. 103/2013 Sb.), zatímco ostatní kriminalitou páchanou v kyberprostoru je *„kriminalita páchaná za výrazného využití informačních a komunikačních technologií, přičemž hlavním objektem útoku je zejména život, zdraví, majetek, svoboda, lidská důstojnost a mravnost“* (Pokyn policejního prezidenta č. 103/2013 Sb.).

Lze předpokládat, že v případném upraveném pokynu policejního prezidenta nebude třeba v daném vymezení těchto forem kriminality činit významnějších změn. I nová NCTEK zůstane s vysokou pravděpodobností i nadále zaměřena hlavně na závažné útoky na kritickou infrastrukturu, případně další významné cíle z hlediska národní a případně mezinárodní bezpečnostní úrovně. Vyplývá to i z rozhovoru pro specializovaný server Lupa.cz, který poskytl náměstek policejního prezidenta pro Službu kriminální policie a vyšetřování Tomáš Kubík. Konkrétně uvedl: *„Dneska se kyberkriminalita, která trápí nejvíc občany, myslím tím případy spoofingu, vishingu a dalších podvodů na internetu, řeší na úrovni obvodních a místních útvarů, protože je tam škoda v přestupkové výši. Je prostě iluzorní, že by takové případy měl řešit speciální útvar z centrální úrovně“* (Vaca 2022).

NCTEK bude s vysokou pravděpodobností i nadále řešit trestné činy páchané formou kybernetických útoků, které mají podle doposud platného povahu kybernetického bezpečnostního incidentu, oznámených Národním úřadem pro kybernetickou a informační bezpečnost, které se vyznačují zvláště sofistikovaným způsobem provedení nebo zvlášť závažným následkem (Pokyn policejního prezidenta č. 103/2013 Sb.). Podle § 7 odst. 2) zákona o kybernetické bezpečnosti je kybernetickým bezpečnostním incidentem *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“* (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti).

Na základě předchozí citace i na základě celkového zaměření NCTEK je třeba zajistit bezproblémovou spolupráci mezi NCTEK a NÚKIB, což se s ohledem na zákonné vymezení i zmíněnou předpokládanou personální kontinuitu mezi NCOZ a NCTEK jeví jako snadno splnitelný požadavek. Důležité samozřejmě bude i udržování vazeb NCTEK na specialisty na kybernetickou kriminalitu v rámci soustavy státního zastupitelství, dominantně pak na Národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost. Ten ve výroční zprávě za rok 2021 vznik specializovaného útvaru požadoval (Foldyna 2022: 6). Je přitom třeba uvést, že druhá – „extremisticko-teroristická“ část NCTEK – má „svého“ Národního korespondenta pro boj proti terorismu, extremismu a trestným činům spáchaným z nenávisti (Lata 2021).

NCTEK musí samozřejmě mít upravené vazby i na zpravodajské služby, zvláště pak BIS vzhledem k jejímu zaměření na specifické kybernetické hrozby a na Vojenské zpravodajství s ohledem na to, že mu bylo v roce 2021 svěřeno „zajišťování cílené detekce kybernetických útoků a hrozeb majících původ v zahraničí a směřujících proti důležitým zájmům státu, identifikace a vyhodnocování takových útoků a hrozeb, jakož i přijímání opatření k jejich odvracení“ (Foldyna 2022: 6).

Na NCTEK by měla fungovat i kvalitní analytika, která umožní identifikovat nejen podstatné trendy ve vývoji kybernetické kriminality a možnosti jejich odhalování (schopnost kvalitní práce v tomto směru ukázaly již dosavadní struktury NCOZ), ale i analyzovat a vyhodnocovat dosavadní českou a evropskou judikaturu, mj. se zaměřením na přípustnost jednolitých důkazů získaných v důsledku mezinárodní spolupráce v trestním řízení.

V rámci samotného NCTEK se nabízí možnost precizovat propojení aktivit specialistů na extremismus a terorismus na straně jedné a specialistů na kyberne-

tickou kriminalitu na straně druhé, a to především ve vztahu ke kybernetickým útokům páchaným příslušníky extremistických entit (Ullah 2017) – ať již organizovaných pouze ve virtuálním prostoru (mj. komunity soudobého tzv. Terrorgramu) anebo i ve fyzickém světě (Kriner, Ihler 2022).

Experti na ICT-technologie pochopitelně budou i nadále poskytovat expertům na extremismus a terorismus součinnost v kontextu identifikace míst (IP adres, reálných připojení apod.), odkud je páchána extremistická a teroristická činnost v kyberprostoru (ve smyslu širšího pojetí, např. zveřejňování manuálů k uskutečňování teroristických útoků). O tom, že kyberprostor (včetně tzv. darkwebu) je intenzivním a v zásadě dominujícím prostorem extremistické a teroristické komunikace a propagandy (včetně tzv. on-line radikalizace), se s ohledem na obecnou známost této skutečnosti není třeba v této studii více rozepisovat. IT-experti pracující pro bezpečnostní složky samozřejmě musí flexibilně reagovat na pokroky extremistů a teroristů ve využívání kyberprostoru, včetně narušování jejich kybernetických bezpečnostních opatření – např. v situaci, kdy levicoví extremisté adorovali používání platformy riseup.net, mělo by to pro bezpečnostní experty státu představovat výzvu ke „zdolání" této překážky (viz citace z webu Sítě revolučních buněk: *„V anarchistickém prostředí je v oblibě e-mailová komunikace přes RiseUp.net, protože tato platforma zaručuje anonymitu a odmítá spolupráci s policií, soudy atd. Často se vedou debaty o tom, zda se můžeme na tuto záruku opravdu spolehnout. Vystává mnoho otázek. Kauza Fénix naštěstí na některé dokázala odpovědět. Přinesla třeba několik příkladů, že policie vážně nedokáže RiseUp.net prolomit a získat citlivé údaje o lidech, kteří využívají jejich služeb"* – Síť revolučních buněk 2018).

Na opačnou stranu, experti na extremismus mohou přispět svými poznatky k odhalování kybernetické kriminality. V extremistických komunitách na domácím území může být kriminální zpravodajství uskutečňováno i formou vytěžování lidských zdrojů (HUMINT). Cílem by mělo být odhalit tzv. insidery, kteří usilují o neoprávněný přístup k počítačovým systémům anebo o jiné páchání kybernetické kriminality na základě extremistického ideového přesvědčení a mohou získat pracovní pozice či alespoň externí přístup k databázím ve státních, soukromých či akademických podnicích a přístupové údaje pak dále zneužívat, šířit svým ideovým spojencům anebo je prodávat za účelem získání prostředků pro vlastní extremistickou entitu.

V rámci působení NCTEK metodického vedení krajských a okresních specialistů na kybernetickou kriminalitu anebo pro podporu prevence je možné na základě poznatků z praxe zpracovat manuály na vytipování lidí, kteří se z důvodu extremistického přesvědčení zapojují do páchání trestných činů kybernetické kriminality. V této souvislosti je jako jistý exkurs a potenciální výchozí model pro další rozpracování třeba zmínit základní přehled extremisticky motivovaných aktérů pro zneužití pozice „insidera" v soukromých společnostech, zpracovaný autorem této studie na základě jeho expertního úsudku do prezentace pro přednášku pro klubový večer ISACA v roce 2021 (Mareš 2021b).

Rozpracování těchto modelů pochopitelně nemůže být hlavní činností NCTEK. Nicméně schopnost identifikovat pachatele kybernetické kriminality prostřednictvím jeho projevů v kyberprostoru i mimo něj je samozřejmě důležitou součástí kriminalistické práce. Výzvou je získávání informátorů v různých hackerských organizovaných zločineckých komunitách, kde si lze představit v případě nejzávažnějších forem kriminality i nasazení policejních agentů podle § 158e trestního řádu (Zákon č. 141/1961 Sb.).

Takovéto přístupy jsou samozřejmě pro PČR reálně uskutečnitelné především na domácím území anebo na území spojeneckých zemí. Je však skutečností, že závažné útoky přicházejí často ze zemí, které jsou chápány jako protivník, respektive nepřítel. NCTEK se reálně bude muset výrazně zabývat i kriminálními činy, jejichž původci jsou zahraniční státní nebo státem řízení aktéři. To se týká i řady potenciálních aktů kyberterorismu.

Schéma č. 1: Motivace extremisticky orientovaných osob ke zneužití pozice insidera pro narušení kybernetické bezpečnosti firmy

Druh extremisty	Důvody ke zneužití pozice insidera pro narušení kybernetické bezpečnosti firmy
Pravicově extremistický insider	Etničtí/rasoví (včetně antisemitismu) političtí oponenti mezi zaměstnanci/vlastníky/partnery organizace + zapojení organizace do projektů „nové levice“
Anarchistický extremistický insider	Obecně odpor ke kapitalismu a autoritám, specificky proti válečnému úsilí Západu a omezování migrace
Komunistický extremistický insider	Vazba na zájmy komunistického hnutí ve světě, odpor ke kapitalismu a Západu, podpora Ruska, Číny, KLDR, Kuby apod.
Environmentalistický/„zvířecko--právní“ extremistický insider	Vazba organizace na poškozování životního prostředí, případně poškozování práva zvířat (specificky vivisekce, množírny, velkochovy)
Náboženský extremistický insider	Jednání organizace a personálu (včetně vnitřních formálních i neformálních norem i vnějších smluvních vztahů) proti zásadám náboženství, u islamistických extremistů specificky zapojení do aktivit pro výraznou svobodu projevu z pohledu insidera urážející islám
Etnický/separatistický extremistický insider	Poškozování zájmů vlastního či spřáteleného etnika/regionu aktivitou organizace, zaměstnanci/vedoucí/partneři subjektivně vnímaných nepřátel etnického/separatistického úsilí

Zdroj: Mareš 2021b

5

KYBERTERORISMUS V KONTEXTU § 311, § 312a A § 313 TRESTNÍHO ZÁKONÍKU

Jednou z hrozeb, před kterou je v zásadě od vzniku internetu a počítačových sítí intenzivně varováno, která ale doposud v užším definičním pojetí nebyla v takové míře intenzity naplněna, je kybernetický terorismus (kyberterorismus). V souvislosti se vznikem nového policejního útvaru i ve vazbě na novelizaci právní úpravy je důležité uskutečnit i právní a bezpečnostní analýzu toho, za jakých okolností by mohl být aplikován § 311 trestního zákoníku (teroristický útok) a následující ve vztahu ke specifické úpravě útoků prostřednictvím kybernetických zařízení.

Nejvíce je z hlediska použité terminologie na kyberprostor zaměřen § 311, odst. 1 písmeno e), v platném znění po zatím poslední novele z roku 2022 (Zákon č. 130/2022 Sb.). Ve spojení s úvodní větou pak příslušné vymezení skutkové podstaty teroristického útoku zní: *„Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla … vložením nebo přenosem dat do počítačového systému nebo na nosič informací, učiněním jiného zásahu do programového nebo technického vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat anebo vymazáním nebo jiným zničením, poškozením, změněním nebo potlačením dat uložených v počítačovém systému nebo na nosiči informací, snížením jejich kvality nebo učiněním jich neupotřebitelnými provede útok proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok anebo útok, kterým způsobí značnou škodu, bude potrestán odnětím svobody na tři až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku“* (Zákon č. 40/2009 Sb.).

Vyšší trest pak může být spojen s kvalifikovanou skutkovou podstatou podle odstavce tři, konkrétně se zde pak uvádí *„Odnětím svobody na dvanáct až dvacet let, popřípadě vedle tohoto trestu též propadnutím majetku, nebo výjimečným trestem bude pachatel potrestán,*

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem těžkou újmu na zdraví nebo smrt,
c) způsobí-li takovým činem, že větší počet lidí zůstal bez přístřeší,
d) způsobí-li takovým činem škodu velkého rozsahu,
e) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu,
f) ohrozí-li takovým činem závažně mezinárodní postavení České republiky nebo postavení mezinárodní organizace, jejíž je Česká republika členem, nebo
g) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu“ (Zákon č. 40/2009 Sb.).

Na vymezení skutkové podstaty v § 311 pak navazuje i § 313, podle kterého se ochrana podle § 311 poskytuje též cizímu státu.

V souhrnu lze tedy konstatovat, že ke spáchání trestního činu teroristického útoku specifickou „kybernetickou (respektive „kyberteroristickou“) formou“ musí být přítomen zaprvé prvek úmyslu (tedy specificky vymezeným způsobem poškodit Českou republiku anebo její obyvatelstvo, případně cizí stát) a zadruhé

prvek použití specifické formy jednání (tedy určitých postupů v kyberprostoru proti jednomu či více počítačovým systémům) a zatřetí prvek závažných dopadů (s ohledem na jazykový výklad zřejmě postačí to, že narušení počítačového systému by mělo uvedený dopad či dopady, ne tedy, že pachatel musí tyto dopady způsobit) anebo jiných závažných následků. Specifické následky pak mohou vést k vyšší trestní sazbě.

Je však třeba mít na paměti, že kybernetický prostor může sloužit i k uskutečnění dalších druhů útoků, zmíněných v trestním zákoníku. Činy vymezené pod písmenem e) v prvním odstavci § 311 směřují dominantně ke zneschopnění počítačového systému, nicméně kyberterorismus může směřovat (v případě adekvátního provedení) i ke zničení, anebo dokonce ovládnutí takových systémů a způsobení dalších škod. V tomto směru je možné uskutečnění kybernetického útoku podle písm. a) odst. 1 anebo písm. c) odst. 2 tohoto paragrafu. Konkrétně se jedná o to, že pachatel *„zničí nebo poškodí ve větší míře veřejné prostranství, majetek nebo veřejné zařízení, dopravní nebo telekomunikační systém, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, včetně počítačového systému, na jehož fungování takové zařízení, systém nebo plošina závisejí“* (Zákon č. 40/2009 Sb.). Počítačový systém lze přitom zničit útokem v kybernetickém prostoru i fyzickým útokem (např. nástražným výbušným systémem, umístěným v místnosti se servery s řídicími programy a příslušnými daty).

V případě získání kontroly nad řídicími počítačovými systémy pak lze spáchat i teroristické útoky podle písm. a) a d) odst. 1 anebo písm. e) a g) odst. 2 tohoto paragrafu (rozdíl spočívá v závažnosti následku a odpovídající výši trestní sazby), konkrétně pak pokud se pachatel *„zmocní letadla, lodi, jiného prostředku osobní či nákladní dopravy nebo pevné plošiny na pevninské mělčině nebo nad takovým dopravním prostředkem nebo pevnou plošinou vykonává kontrolu anebo zničí nebo vážně poškodí navigační zařízení nebo ve větším rozsahu zasahuje do jeho provozu“* (Zákon č. 40/2009 Sb.) anebo pokud pachatel (při způsobení zákonem stanoveného závažného následku, přičemž stačí ohrožení) *„způsobí požár nebo povodeň nebo škodlivý účinek výbušnin, plynu, elektřiny nebo jiných podobně nebezpečných látek nebo sil nebo se dopustí jiného podobného nebezpečného jednání, nebo takové obecné nebezpečí zvýší nebo ztíží jeho odvrácení nebo zmírnění“* (Zákon č. 40/2009 Sb.).

V zásadě teprve jednání uvedená v předchozím odstavci by naplňovala znaky kyberterorismu v jeho užším pojetí, do mírně širších definic kyberterorismu by pak spadala i jednání uvedená pod písmenem e).

Pachatelé těchto forem kyberterorismu přitom mohou být nestátní i státní aktéři, tzn., že i příslušníci vojenských složek mohou být odpovědni za takovéto činy. V trestním zákoníku přitom není explicitně zmíněno, že by bylo použití těchto paragrafů vyloučeno za válečného konfliktu, nicméně orgány činné v trestním řízení by mohly v takovém případě argumentovat odkazem na mezinárodní právo. V zásadě totiž jinak lze velkou část kybernetických útoků za válečného konfliktu páchaného proti zájmu chráněnému zákonem podřadit pod výše uvedený paragraf § 311, protože i v případě útoku proti vojenským cílům naplňují požadovaný znak úmyslu poškodit obranyschopnost České republiky.

Ještě větší otázky pak vyvolává aplikace tohoto paragrafu na ochranu cizího státu podle § 313. V této souvislosti je třeba klást důraz na adekvátnost takové ochrany ve vztahu k § 12 odst. 2 trestního zákoníku, kde se uvádí, že trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých, ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu“ (Zákon č. 40/2009 Sb.). V daném kontextu je možné debatovat o tom, zda například hackerské akce ukrajinských útočníků proti Rusku či běloruských emigrantů proti režimu Alexandra Lukašenka naplňují kritérium společenské škodlivosti, či zda je naopak spíše není třeba chápat jako společensky prospěšné. Obecně by určité státy měly ztratit ochranu podle trestního zákoníku či její část, pokud je jejich politika na základě politických rozhodnutí cíleně zaměřena proti bezpečnostním zájmům ČR a vůči ČR jsou uskutečňovány tímto cizím státem podporované či státem přímo vykonávané subversivní aktivity.

Na straně druhé je zde samozřejmé hrozba, a to jak v kybernetické oblasti, tak ve světě, že tolerance vůči kybernetickým útokům povede k odvetným krokům, a to nejen recipročním, ale i k vystupňování konfliktu. Nezávislost soudů v rozhodování je samozřejmě mimořádně důležitým prvkem demokratického právního státu, je však přičitatelná jako jednání státu navenek, a tuto skutečnost je třeba mít na paměti při tvorbě bezpečnostní politiky.

Další právní výzva v této oblasti trestního zákoníku se týká teroristických skupin, které by páchaly výše skutkové podstaty v § 311, a to s ohledem na další ustanovení trestního zákoníku, konkrétně pak § 312a a účast na teroristické skupině. Trestná je i samotná účast na teroristické skupině, když je v prvním odstavci § 312a uvedeno: *„Kdo založí teroristickou skupinu nebo kdo se činnosti teroristické skupiny účastní, bude potrestán odnětím svobody na tři až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku“* (Zákon č. 40/2009 Sb.). Ve druhém odstavci je pak uvedeno, že *„odnětím svobody na pět až patnáct let, popřípadě vedle tohoto trestu též propadnutím majetku, bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a) jako vedoucí činitel nebo představitel teroristické skupiny, nebo b) jako zakladatel nebo člen teroristické skupiny, která naplňuje znaky organizované zločinecké skupiny“* (Zákon č. 40/2009 Sb.).

Teroristickou skupinou se přitom ve smyslu § 129a trestního zákoníku myslí společenství *„nejméně tří trestně odpovědných osob, které má trvalejší charakter, je v něm provedena dělba činností mezi jeho jednotlivé členy, jeho činnost se vyznačuje plánovitostí a koordinovaností a je zaměřeno na páchání trestného činu vlastizrady spáchané formou teroristického útoku nebo teroru (§ 309), trestného činu teroristického útoku (§ 311) nebo trestného činu teroru (§ 312)“* (Zákon č. 40/2009). Organizovaná zločinecká skupina je v § 129 definována jako společenství *„nejméně tří trestně odpovědných osob s vnitřní organizační strukturou, s rozdělením funkcí a dělbou činností, které je zaměřeno na soustavné páchání úmyslné trestné činnosti“* (Zákon č. 40/2009 Sb.).

Doposud nebyla tato právní úprava aplikována v žádném případě, který by se týkal výhradně kybernetického terorismu, pouze v několika případech byla brána do úvahy komunikace a propagace některých osob obviněných z účasti na činnosti teroristické skupiny (např. v případě Omara S., který bojoval v rámci teroristické organizace An-Nusra) (Nejvyšší soud České republiky 2021), které v některých případech posloužily i jako důkaz pro teroristickou činnost (např. v případě Alexeje F., který bojoval v řadách Republikánské gardy Doněcké lidové republiky) (Nejvyšší soud České republiky 2022).

V případě Omara S. soud mj. konstatoval: *„Ze zajištěné četné komunikace mezi obviněnými navzájem i mezi obviněnými a jejich rodinnými příslušníky přes aplikace Whatsapp a Telegram jednoznačně vyplývá, že dovolatel působil v organizaci nejméně do října 2017. V této emailové komunikaci a audiozprávách je trestná činnost obviněného detailně popsána od vylíčení cesty do Sýrie přes účast ve výcvikovém vojenském táboře, kurzy, sňatek se spoluobviněnou F. H., až po jejich konkrétní zapojení do činnosti uskupení An-Nusra. Vzájemná komunikace obviněných je natolik rozsáhlá a podrobná, že její obsah nelze zpochybňovat“* (Nejvyšší soud České republiky 2021). V případě Alexeje F. pak videosoubory ze sociálních sítí dokumentovaly jeho bojovou činnost v řadách tzv. doněckých separatistů (Nejvyšší soud České republiky 2022).

Jak již bylo konstatováno, v těchto případech důkazy z kyberprostoru posloužily „pouze“ jako důkaz k prokázání činnosti ve skupinách, které činnosti, jež byly posouzeny jako teroristické útoky, páchaly převážně ve fyzickém světě. Nicméně do úvahy připadá i vymezení teroristické skupiny anebo organizované zločinecké skupiny, které by byly zaměřeny na páchání kybernetických teroristických útoků.

V této souvislosti lze uvažovat o dvou typech organizací, a sice o

1) teroristických skupinách, které páchají kybernetické teroristické útoky dominantně ve fyzickém světě a kybernetický terorismus je jistým „doplňkem“ nebo i důležitou součástí jejich činnosti (příkladem může být Hizballáh);

2) teroristických skupinách, které jsou zaměřeny pouze na kybernetickou teroristickou činnost (příkladem mohou být různé hackerské kolektivy schopné teroristických útoků, např. ruský DarkSide – pokud nebude chápán jako součást ruských tajných služeb zaměřených i na „fyzickou“ teroristickou činnost) (Jacobsen 2022: 64).

V případě druhé uvedené kategorie je možné v hmotněprávní rovině podle mého názoru aplikovat i výše zmíněné § 129 a § 129a trestního zákoníku. Organizovaná zločinecká skupina přitom vyžaduje více rigidní strukturu než teroristická skupina. U organizované zločinecké skupiny jsou důležitými elementy právní definice počet nejméně tří právně odpovědných osob, soustavnost páchání trestné činnosti, vnitřní organizační struktura, rozdělení funkcí a dělba činnosti. V případě, že bude například ve skupině rozdělena role v prolomení kódu, na tomto základě jiným členem bude zneužito ovládání prostřednictvím digitalizovaných zařízení (např. energetické soustavy) a následně

budou další členové blokovat snahy protivníka o znovuzískání kontroly nad zařízením, bude se jednat o dělbu činnosti i rozdělení funkcí, je přitom otázkou, zda organizace může být i lineární (tedy členové budou například přijímat rozhodnutí kolektivně – dle mého názoru ano). Znaky teroristické skupiny jsou rovněž tři osoby (právně odpovědné), postačí trvalejší charakter (nikoliv tedy soustavné páchání trestné činnosti), dělba činnosti, plánovanost a koordinovanost a zaměření na konkrétní trestné činy. I kolektiv, který se zorganizuje a bude provádět kyberteroristický útok z více míst, bude naplňovat znaky vyžadované trestním zákoníkem.

Sporné může být určení názvu a vymezení takové teroristické skupiny. Může se například jednat o uskupení sestávající z pracovníků státní tajné služby či jí najatých či ovládaných útočníků (ty obvykle dostávají jména od vnějších aktérů), případně o nestátní nepojmenovaný kolektiv či kolektiv udržující vlastní název neveřejný. Pokud skupina vydává vlastním jménem komuniké k vysvětlení své činnosti, je určení názvu v případě dostatečné důkazní schopnosti přiřknout útok snadné. Nicméně se někdy může jednat i o útok pod falešnou vlajkou (pak je třeba jasné přiřčení). Sporné může být i obecné vymezení názvu, který si nárokuje řada často protikladně zaměřených kolektivů – typické je to například pro Anonymous, jejichž značku využívají různí aktéři, dnes již bez jasného jednotícího prvku. Jak uvádí Jeppe T. Jacobsen, za Anonymous se dnes označují různě technicky vybavení *„hackeři, nerdi, spammeři, aktivisté a sexuální devianti“* (Jacobsen 2022: 67). Právní určení konkrétní kyberteroristické skupiny tedy zůstává výraznou výzvou pro orgány činné v trestním řízení a bude je třeba upřesnit i judikaturou.

6

KYBERNETIČTÍ ZAHRANIČNÍ BOJOVNÍCI V KONTEXTU § 321 A § 321a TRESTNÍHO ZÁKONÍKU

Kromě účasti v teroristických skupinách je současnou právní výzvou i potenciální postih kybernetických bojovníků podle § 321 služba v ozbrojených silách a případně i podle § 321a účast na nestátní ozbrojené skupině zaměřené na působení v ozbrojeném konfliktu. Obě skutkové podstaty se do trestního zákoníku dostaly především s ohledem na válčení ve fyzické dimenzi, z hlediska ČR především v pozemních vojscích cizích států a nestátních entit (Mareš, Výborný 2015). Poté co se postih za službu v nestátních silách ukázal jako problematický, pokud nešlo o účast na činnosti teroristické skupiny (Richterová 2021: 145–158), byla v roce 2022 přijata výše zmíněná nová skutková podstata zaměřená na tuto problematiku. Jedním z důvodů byla v některých případech obtížná i rozlišitelnost mezi státním a nestátním charakterem ozbrojených uskupení (Parlament České republiky. Poslanecká sněmovna 2021: 25).

V současné době lze tedy v trestním zákoníku v ČR nalézt § 321 „Služba v cizích ozbrojených silách", kde se uvádí: *„(1) Občan České republiky, který v rozporu s jiným právním předpisem koná službu ve vojsku nebo ozbrojených silách jiného státu, bude potrestán odnětím svobody až na pět let. (2) Odnětím svobody na tři léta až deset let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 za stavu ohrožení státu nebo za válečného stavu"* (Trestní zákoník č. 40/2009 Sb.). Na něj navazuje nový paragraf § 321a Účast na nestátní ozbrojené skupině zaměřené na působení v ozbrojeném konfliktu: *„Kdo se účastní činnosti nestátní ozbrojené skupiny zaměřené na působení v ozbrojeném konfliktu probíhajícím na území jiného státu tím, že a) se zapojí do bojové činnosti takové skupiny, b) jinému poskytne informace nebo výcvik týkající se výroby nebo používání výbušnin, zbraní, nebezpečných látek nebo materiálů obdobné povahy anebo jiných obdobných metod nebo technik za účelem spáchání činu uvedeného v písmenu a), c) získá informace nebo si osvojí dovednosti týkající se výroby nebo používání výbušnin, zbraní, nebezpečných látek nebo materiálů obdobné povahy anebo jiných obdobných metod nebo technik za účelem spáchání činu uvedeného v písmenu a) nebo b), nebo d) cestuje do jiného státu nebo do České republiky za účelem spáchání činu uvedeného v písmenu a), b) nebo c), bude potrestán odnětím svobody až na pět let"* (Trestní zákoník č. 40/2009 Sb.).

Jiným právním předpisem dle § 321 je § 34 zákona č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon). V něm je uvedeno následující

„1) Občan smí vstoupit do ozbrojených sil jiných států pouze se souhlasem prezidenta republiky na základě své žádosti, nestanoví-li tento zákon jinak.

2) Občan žádost o souhlas prezidenta republiky se vstupem do ozbrojených sil jiného státu podává ministerstvu, které ji se svým vyjádřením a po projednání s Ministerstvem vnitra a Ministerstvem zahraničních věcí předloží prezidentovi republiky. Občan v žádosti uvede kromě obecných náležitostí podání podle správního řádu také rodné číslo.

3) Souhlas prezidenta republiky pozbývá platnosti dnem účinnosti vyhlášení stavu ohrožení státu nebo válečného stavu. Na udělení souhlasu není právní nárok.

4) Občan, který má více státních občanství, může vstoupit do ozbrojených sil jiného státu, jehož je také státním občanem, bez souhlasu prezidenta republiky. Bez souhlasu prezidenta republiky může vstoupit do ozbrojených sil jiného státu též občan

za předpokladu, že tento stát je členem mezinárodní organizace zajišťující společnou obranu proti napadení, jíž je Česká republika členem.

5) Prezident republiky může za stavu ohrožení státu nebo za válečného stavu vyzvat vojáky v záloze, kteří jsou v zahraničí, aby vstoupili do ozbrojených sil spojeneckého státu, na jehož území se nacházejí nebo do něhož se mohou dostat. Vojenská služba takto vykonaná se považuje za mimořádnou službu" (Zákon č. 585/2004 Sb.).

Z hlediska kybernetických bojovníků je třeba mít na paměti důležitou skutečnost, že svoje úkoly mohou plnit i daleko od místa konfliktů ve fyzickém světě, včetně svého domova. Na straně druhé může být z vojenského hlediska důležité i jejich soustředění na konkrétním místě, ať již z hlediska efektivnější koordinace a dohledu anebo vhodného přístrojového a softwarového vybavení. A naopak, za určité situace je vhodná pozice insidera s přístupem na síť v prostoru, který kontroluje protivník, včetně velicích center protivníka, jeho zbrojních zařízení, vládních institucí apod. Pokud by takový protivník působil přímo proti objektům ČR (včetně působení na jejím území), byl by občan působící v jeho prospěch kybernetickým bojem postižitelný podle různých skutkových podstat v trestním zákoníku (např. § 361 účast na organizované zločinecké skupině), včetně § 309 vlastizrady. V takovém případě by bylo pouze doplňujícím poznatkem (byť za určité situace využitelným pro dokázání jiných trestných činů či jako přitěžující okolnost) to, zda je členem ozbrojených sil cizího státu nebo nestátní skupiny (která by byla tzv. cizím činitelem).

Lze si však představit i situaci, kdy bude v ozbrojených silách anebo v nestátní entitě působit i občan České republiky, který bude součástí kybernetických bojových sil zapojených do konfliktu, a tento konflikt nebude přímo zasahovat ČR. Současně nepůjde z hlediska výkonu služby takového občana o spojenecký stát vázaný k ČR smlouvou o společné obraně ve smyslu čtvrtého odstavce § 34 branného zákona a takový občan nebude mít ani výjimku od prezidenta republiky podle téhož zákona. V takovém případě se jedná o jednání, které je trestné podle trestního zákoníku, samozřejmě za splnění podmínky společenské škodlivosti dle druhého odstavce § 12 trestního zákona). Ve vztahu k § 321a je pak třeba uvést, že na rozdíl od § 321 není u nestátní ozbrojené skupiny možný souhlas prezidenta.

Zásadním znakem dle § 321 je to, aby pachatel sloužil v cizím vojsku nebo ozbrojených silách jiného státu (výjimky viz výše). Důležitý je proto určitý kontrakt či vědomý akt vázanosti k ozbrojeným silám takového státu, zpravidla tedy i získání hodnosti, funkce apod. Pokud by takovou pozici získal člověk provádějící kybernetické útoky, mohl by podle mého názoru naplnit skutkovou podstatu podle § 321 TZ. I případné nenošení uniformy pak není podstatné, protože je vázáno na jiné normy, respektive jejich porušování. U § 321a je vyžadována ozbrojenost skupiny a je otázkou, zda za takovou zbraň budou uznány i kybernetické zbraně. Dle mého názoru mohou být, nicméně to není potvrzeno judikaturou. Pokud by nicméně jako takové byly uznány, pak lze i čistě nestátně kyberneticky působící skupiny využívající kybernetické zbraně chápat ve smyslu tohoto paragrafu a v daném kontextu i postih zde popsaných jednání podle písmen a) až d). Navíc si lze představit i zapojení do bojových úkolů skupiny působící i v klasickém boji ve fyzickém světě formou kybernetické podpory takového boje, tedy že skupina bude kombinovat tradiční konvenční a kybernetický boj a pachatel se zapojí do toho kybernetického.

Jak již bylo uvedeno, u kybernetické války má specifickou roli teritorialita, protože není nutná fyzická účast na místě konfliktu. V § 321a je vyžadováno zaměření skupiny na působení v ozbrojeném konfliktu probíhajícím na území jiného státu, nicméně to neznamená, že by kybernetický boj ve prospěch takové skupiny nemohl probíhat i na jiném místě. V zásadě si lze představit, že jak v případě § 321a, tak i § 321 bude pachatel působit

1) v cizím státě, kde konflikt probíhá, přímo v místě bojových operací (jeho kybernetická činnost pak může být např. doplňkem elektronického boje);

2) v cizím státě, kde konflikt probíhá, ale mimo hlavní zónu fyzických bojových operací (například v dostatečně technologicky vybaveném kybernetickém centru);

3) na území jiného státu, než probíhá konflikt, i mimo ČR (například z důvodu soustředění ideově spřízněných hackerů-členů skupiny v zemi, kde mají klidné zázemí);

4) na území ČR (pokud takovou kybernetickou bojovou činnost připojení z ČR umožňuje).

Je přitom třeba ještě jednou zdůraznit, že výše zmíněná analýza obou paragrafů (§321 a § 321a) je z hlediska účasti kybernetických bojovníků mým autorským náhledem a není dosud podpořena judikaturou, a pokud je mi známo, ani jiným odborným výkladem. O kybernetické dimenzi bojovníků v nestátních skupinách nehovoří ani důvodová zpráva k novele (Parlament České republiky. Poslanecká sněmovna 2021).

Do budoucna (ale v zásadě i v současnosti) se může jevit jako vysoce citlivou záležitostí i případný postih občanů ČR, kteří mají dvojí občanství některého z nedemokratických zahraničních států a působili by na území ČR v zásadě jako součást „kyberpartyzánských skupin“ (například útočících na běloruskou dopravní infrastrukturu, využívanou ruskými vojsky k agresi proti Ukrajině), případně českých občanů, kteří by takové činnosti napomáhali (i osobám bez českého občanství). Zde by měly orgány činné v trestním řízení zvážit již zmíněné ustanovení o společenské škodlivosti dle § 12 trestního zákoníku, případně by to měla být výzva pro zákonodárce, aby zvážil adekvátní úpravu trestního zákoníku či jiných právních norem umožňujících vyvinění těch, kteří v takových strukturách s celkově pozitivním dopadem ve vztahu k bezpečnostním zájmům ČR působí.

7

AKTUÁLNÍ TRENDY VE VYBRANÝCH DALŠÍCH FORMÁCH KYBERNETICKÉ KRIMINALITY

Zatímco výše analyzované skutkové podstaty v trestním zákoníku nepatří k těm nejvíce frekventovaným, potýkají se orgány činné v trestním řízení i další bezpečnostní složky v ČR s více „tradičními" formami kybernetické kriminality. Pokud vyjdeme ze zprávy národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost na NSZ za rok 2021, pak lze za tento rok pozorovat nárůst kriminality v kyberprostoru i kybernetické kriminality v užším slova smyslu, přestože jinak celková úroveň všech druhů kriminality (zřejmě i v důsledku pandemie) klesla (Foldyna 2022: 2).

Podle téže zprávy výrazně narostly podvody v kyberprostoru, a to jednak využívající falešné identity podvádějícího, který pod touto identitou (např. amerického vojáka navracejícího se z mise) navazuje zdánlivě intimní vztah s obětí, od které vymámí pod různými záminkami peníze, a jednak výzvami k nákupu kryptoměn, při kterém je ale kupující okraden (Foldyna 2022: 3). Národní korespondent rovněž konstatoval nárůst hackingu a také pokles ransomwarových útoků oproti roku 2022 (Foldyna 2022: 3). Je přitom třeba uvést, že v roce 2019 a zvláště v roce 2020 představovaly ransomwarové útoky, zvláště na nemocnice a další zdravotnická zařízení, závažnou hrozbu, vůči které však byla postupně přijímána adekvátní protiopatření a podařilo se i napravit některé škody a uvést systémy do provozu (Mareš 2021a).

V letech 2021 a 2022 se výrazně zvýšil i počet tzv. vishingových útoků. Podle výkonné ředitelky České bankovní asociace Moniky Zahálkové údajně každý druhý telefonát skončil škodou pro klienta (Česká bankovní asociace 2022: 2). Podle Policie ČR přitom bývá vishing – tedy telefonický hovor, ve kterém se pachatel falešně představí jako zaměstnanec banky a láká pod vymyšlenou legendou o ohrožení z oběti přístupové údaje ke kontu anebo ho přiměje převést peníze na pachatelem kontrolované konto – doprovázen v současnosti i spoofingem, tedy napodobováním telefonních čísel, včetně čísla bankovní infolinky, osobního bankéře apod. (Policie ČR 2021).

V rámci úžeji pojaté kyberkriminality s možným přesahem do cizími státy podporované či organizované kriminality se v poslední době zvyšuje počet tzv. DDoS útoků (zkratka Distributed Denial of Service). Podle NÚKIB se tyto útoky vyhrotily na podzim roku 2022 v návaznosti na geopolitickou situaci na východě Evropy a k několika těmto útokům se přihlásila skupina Anonymous Russia, zatímco v dubnu 2022 na ČR útočila jiná ruskojazyčná skupina Killnet (Národní úřad pro kybernetickou a informační bezpečnost 2022c). V této souvislosti je třeba možné opětovně upozornit na obtížnou přičitatelnost útoků a na to, že pod hlavičkou Anonymous vystupují dnes různé kolektivy, ideově často protikladné (možné jsou i operace tajných služeb pod vlajkou Anonymous).

Jak uvádí expert na kyberbezpečnost Jakub Drmola, lze Distributed Denial of Service volně přeložit jako „rozptýlené odepření služby" (Drmola 2012: 4). V překladu jiných autorů se objevuje pojem „distribuované odmítnutí služby" (Jirásek, Novák, Požár 2022: 53). Dle Drmoly je *„cílem těchto útoků typicky server, který svým uživatelům poskytuje nějakou službu (nejčastěji webové stránky, ale může jít například i o elektronické bankovnictví). Záměrem útočníků je tuto službu odepřít či „znepřístupnit" legitimním uživatelům a tím třeba poškodit napadeného poskytovatele služby nebo upozornit na své politické stanovisko"* (Drmola 2012: 4). Tentýž autor dále konstatuje, že útok *„v zásadě*

probíhá pomocí zahlcení napadeného serveru extrémním množstvím digitálních informací a požadavků. Server pak nedokáže zpracovávat legitimní data od běžných uživatelů a těm se pak případná webová stránka zobrazí jako nedostupná, nebo jim služba byla odepřena, Denial of Service" (Drmola 2012: 4). K provedení útoku Drmola uvádí, že k němu dochází ve formě zasílání dat na „cíl" a k tomu *„bývá obvykle užíváno větší množství počítačů, útok je proto distribuovaný,* rozptýlený. K tomu může být využit botnet" (Drmola 2012: 4). Konečně botnet pak chápe jako *„síť počítačů, která může být bez vědomí jejich legitimního majitele a správce vzdáleně využívána k provádění útoků dle kontroly ‚botmastera'. Tyto sítě mohou sestávat až ze stovek tisíc individuálních počítačů, přičemž se většinou jedná o počítače firemní a špatně chráněné. Jejich tvorba bývá výsledkem činnosti malware (většinou červů), který se rozšíří po rozsáhlé a neadekvátně zabezpečené firemní síti a umožní jejich vzdálenou kontrolu"* (Drmola 2012: 9).

V současnosti jsou jako vysoce rizikové hodnoceny kybernetické útoky na dodavatelské řetězce. Obecně dodavatelský řetězec obsahuje *„soubor organizací s propojeným souborem zdrojů a procesů, z nichž každá vystupuje jako dodavatel, nabyvatel nebo obojí"* (Jirásek, Novák, Požár 2022: 52–53). Dodavatelské řetězce obecně mohou být zasaženy různými druhy kybernetických útoků, a ty mohou být směřovány na jednu či více součástí řetězce. Podstatný je následek, kdy může dojít k omezení funkčnosti či k úplnému zhroucení řetězce jako takového. Evropská unie začala klást důraz i na spolehlivost výběru dodavatelských řetězců informačních a komunikačních technologií tak, aby v nich nefigurovali rizikoví dodavatelé a subdodavatelé (Rada Evropské unie 2022).

V souvislosti s dalšími druhy kriminality je možné očekávat ve vazbě na polarizaci společnosti a možný nárůst kriminality některých skupin obyvatelstva i výraznější nástup kybernetického či digitálního vigilantismu, ať již v širším pojetí zveřejňování informací o kriminálním či deviantním jednání konkrétních osob v kyberprostoru anebo v užším pojetí na konkrétní stránky a zařízení osob a entit, chápaných vigilantisty jako nepřátelské (Mareš, Bjørgo 2019: 14).

S ohledem na rozvoj šíření dezinformací a nenávistných projevů na internetu se projevuje stále intenzívněji význam robotické propagandy (Pavlíková, Mareš 2018) a lze očekávat i výraznější využití umělé inteligence na tomto poli. Jak již bylo konstatováno: *„U všech technik robotické propagandy je důležité z právního hlediska stanovit odpovědnost za výslednou činnost. Tu v rámci vnitrostátního práva bude mít osoba či osoby, která či které příslušnou propagandu ideově a technicky (s vědomím jejího účelu) iniciovaly, ať již přímo nebo prostřednictvím spoluúčasti (pokyny, výpomoc apod.). Může se pochopitelně jednat o zahraniční fyzické i právnické osoby"* (Pavlíková, Mareš 2018: 22).

Pokud se týká obecných problémů orgánů činných v trestním řízení při dokazování kriminality v kyberprostoru, konstatoval příslušný národní korespondent na NSZ, že právní vývoj zaostává za technologickým vývojem zneužívaným kriminálníky (zvláště v oblasti šifrování) a přímo uvedl: *„Zatímco šifrování, využívání kryptoměn, používání biometrie k ověřování přístupů a transakcí je již dnes standardem, stejně jako ukládání dat ve vzdálených úložištích, právní rámce jednotlivých zemí i EU jako celku si neví rady, jak tuto problematiku regulovat, takže orgány činné v trestním řízení narážejí na limity spočívající v nemožnosti opatření některých dat pro účely trestního řízení, neboť nemají právní nástroje, jak tyto data získat. Problémy při nastavení právního rámce regulace této oblasti jsou dány především konfliktem mezi potřebami orgánů činných v trestním řízení pronikat do soukromí uživatelů při objasňování těchto forem trestné činnosti a mírou zajištění ochrany základních práv a svobod těchto uživatelů, zvláště pak mírou ochrany jejich soukromí při užívání informačních technologií. Stále více se tak ukazuje být problematickým současný nedostatečný právní rámec, který neukládá poskytovatelům povinnost registrovat údaje o využití služeb VPN, šifrování atd., což vede k tomu, že řada pachatelů závažných trestných činů zůstává skryta v anonymním prostředí internetu nebo darknetu"* (Foldyna 2022: 4).

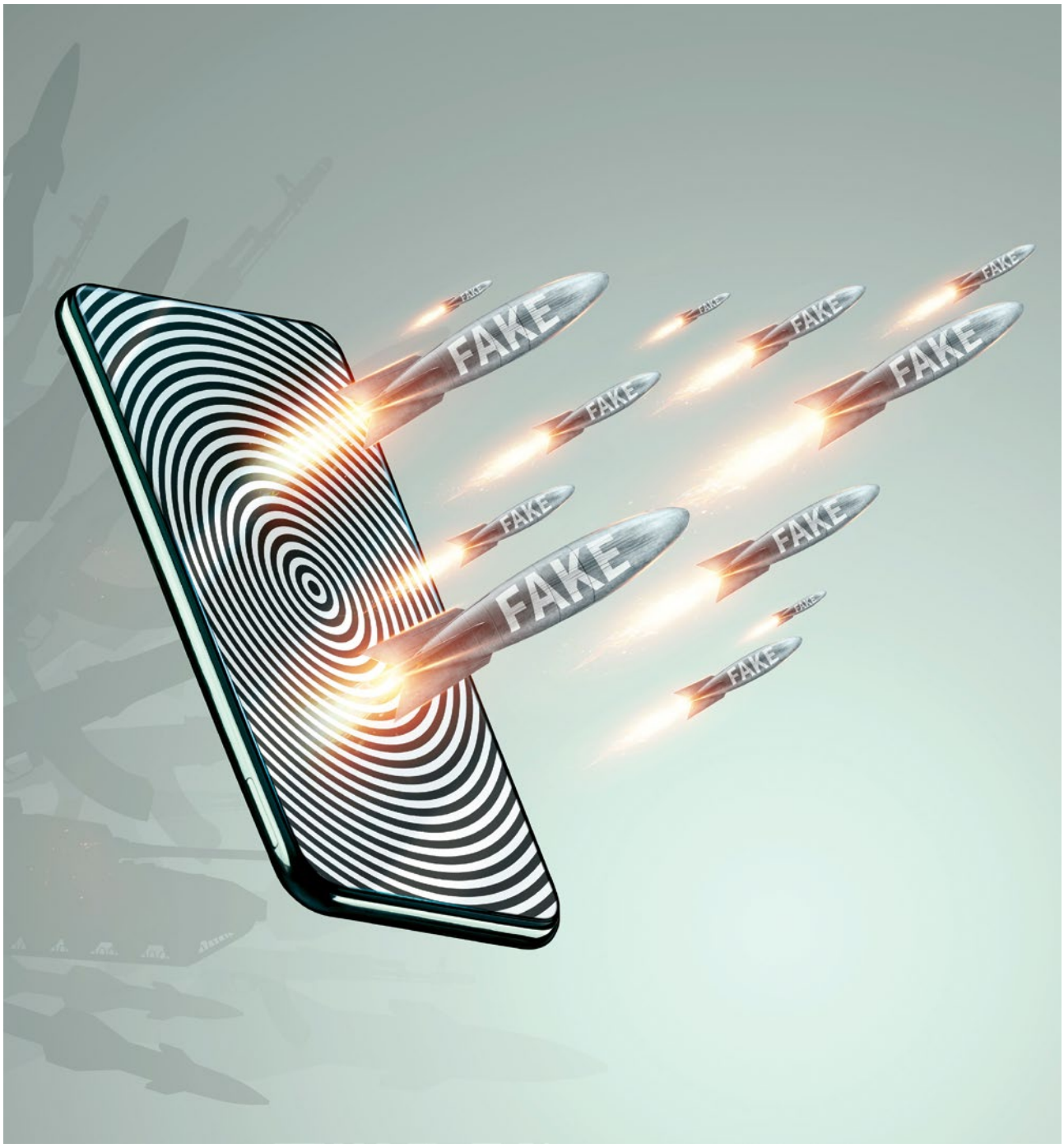
V této souvislosti je třeba uvést, že v současné době se zde ze strany České republiky i ze strany EU nabízí možnost, jak prosadit určité sjednocující prvky do mezinárodního práva, a to díky přípravě komplexní mezinárodní úmluvy o boji proti využívání informačních a komunikačních technologií pro účely trestné činnosti. Jak vyplývá z materiálu Evropské komise, v roce 2019 přijalo Valné shromáždění OSN rezoluci 74/247, kterou byl zřízen otevřený ad hoc mezivládní výbor pro vypracování dané úmluvy a tato rezoluce uvádí, že *„výbor ad hoc má plně zohlednit stávající mezinárodní nástroje a úsilí na vnitrostátní, regionální a mezinárodní úrovni v oblasti boje s využíváním informačních a komunikačních technologií pro účely trestné činnosti, zejména práci a výsledky mezivládní skupiny odborníků"* (Evropská komise 2022).

Výbor začal jednat v roce 2022 a pracuje pod kuratelou Úřadu OSN pro drogy a kriminalitu (UNODC). Doposud proběhla tři z plánovaných šesti kol jednání (předcházela jim však ještě dvě organizační kola), další tři jsou plánovány na rok 2023 s plánovaným ukončením 1. září 2023 (United Nations Office on Drugs and Crime 2022). Úmluva má mít následující strukturu:

„1. Obecná ustanovení, 2. Kriminalizace, 3. Procesní opatření a vymáhání práva, 4. Mezinárodní spolupráce, 5. Technická pomoc, včetně výměny zkušeností. 6. Preventivní opatření. 7. Mechanismus realizace, 8. Závěrečná ustanovení“ (Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes nedat.).

S ohledem na aktuální dění a na prokázané případy i podezření ohledně činnosti kriminálních struktur autorizovaných některými státy k subverzi proti jiným státům by měla úmluva obsahovat jasně vymezený zákaz a sankce vůči takovému jednání. Měly by být nalezeny efektivní mechanismy spolupráce při vyšetřování takového jednání, včetně shody na formě efektivních důkazů přičitatelnosti. O uznání důkazních prostředků by měla být nalezena shoda ve všech oblastech kriminality.

Do budoucna je pro Českou republiku i pro mezinárodní společenství či alespoň pro spojenecké organizace a aliance nutné najít i vhodné způsoby vyšetřování kybernetických zločinů spáchaných za války, kdy bude systém kybernetické bezpečnosti a kybernetické obrany přehlcen množstvím úkolů. Do úvahy je možné brát i výpadky funkčnosti částí sítě či veřejného internetu celkově, a to například v důsledku válkou způsobeného blackoutu (ten mohou alespoň zčásti způsobit i kybernetické útoky). Zajištění důkazů (např. o přičitatelnosti útoků) za takového stavu bude vyžadovat specifickou kriminalistickou práci v kyberprstoru i ve fyzickém světě.


FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE

8

ZÁVĚR

Jak vyplynulo z celé studie, je kybernetická bezpečnost výraznou součástí celkového bezpečnostního systému České republiky, včetně jeho propojení s mezinárodním bezpečnostním systémem. Jak se ukázalo, ČR musí reagovat na nové bezpečnostní požadavky stanovené Evropskou unií (aktuálně zvláště NIS2), případně dalšími mezinárodními organizacemi, i na vlastní vyhodnocení bezpečnostních hrozeb a přijmout adekvátní opatření na tomto poli.

Nové instituce v rámci domácího bezpečnostního systému musí efektivně naplnit a rozvíjet roli, která je jim svěřena. Je však třeba zdůraznit i to, že při reálném začleňování poradce pro národní bezpečnost i Národní centrály proti terorismu, extremismu a kybernetické kriminalitě do bezpečnostního systému ČR je třeba ze strany politických činitelů i veřejnosti určitá míra trpělivosti i tolerance, protože teprve praktické zkušenosti ověří efektivnost vybraných kompetencí a úkolů.

Jak se v celé studii ukazovalo, důležitou roli má multioborový přístup ve výzkumu i v praktické realizaci kybernetické bezpečnosti a kybernetické obrany. Je zřejmé, že pro ITC-oblast kyberbezpečnosti je třeba mít vyškolené programátory i specialisty z informatických oborů, nicméně potřebné jsou i jejich odpovídající znalosti managementu, zpravodajských a bezpečnostních studií a práva, přičemž ze všech těchto oborů je třeba dodávat odpovídající background od expertů, kteří svůj zájem zaměřují alespoň částečně na kybernetickou bezpečnost.

V daném kontextu je třeba vnímat i vybrané problémy představené v této studii, kdy s ohledem na vzdělání a odbornou činnost autora byly analyzovány a doporučovány především záležitosti podložené expertními znalostmi v oblasti politologicky zaměřených bezpečnostních studií a práva. U všech hmotně-právních závěrů (týkajících se mj. kyberterorismu anebo kybernetických zahraničních bojovníků) je třeba čekat na jejich případné potvrzení judikaturou a rovněž je třeba zajistit adekvátní důkazy k prokázání takové trestné činnosti. K tomu bude opět třeba schopných ITC-expertů.

Multioborová realita vyžaduje i nadále kvalitní a rozsáhlý multioborový výzkum v oblasti kyberbezpečnosti. Ten je již v ČR poměrně silně podporován a je třeba v nastaveném trendu pokračovat. Do podpory kybernetické bezpečnosti se vlastní činností mohou a mají zapojovat i politické think-tanky, a proto je třeba na závěr ocenit i zájem Pravého břehu – Institutu Petra Fialy o dané téma, ke kterému mi bylo umožněno napsat tuto studii. Byl bych velmi rád, kdyby našla odezvu u těch, kteří tuto problematiku profesně řeší, i u zájemců z řad širší veřejnosti.

9

LITERATURA A ZDROJE

Bastl, Martin (2008): Budoucnost nekonvenčních forem boje. Rexter, roč. 5, č. 2, s. 53–61.

Bastl, Martin – Gruberová, Zuzana (2013): Kyberprostor jako „pátá doména"?, Vojenské rozhledy, roč. 22 (54), č. 4, s. 10-21.

Brokeš, Filip (2019): Kauza Huawei v Česku: Jak se vlk nažral, a koza zůstala celá. Respekt. Dostupné z https://www.respekt.cz/spolecnost/kauza-huawei-v-cesku-jak-se-vlk-nazral-a-koza-zustala-cela

Council of Europe (2022): Council conclusions on a Framework for a coordinated EU response to hybrid campaigns. Dostupné z https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

Csonka, Peter (2006): The Council of Europe's Convention on cyber-crime and other European initiatives, Revue internationale de droit pénal, roč. Vol. 77, č. 3–4, s. 473–501. Dostupné z https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm

Česká bankovní asociace (2022): Hackerských útoků přibývá, každý třetí Čech se s nimi setkal letos. Česká bankovní asociace News, č. 22, s. 2–3. Dostupné z https://cbaonline.cz/upload/2467-cba-news-22-2022-cz.pdf

IECISO/IEC TS 27100:2020 (2020): Information technology – Cybersecurity – Overview and concepts. Dostupné z https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en

Dolníček, Lukáš (2013): Rozhovor: Vladimír Rohel, Národní centrum kybernetické bezpečnosti, roč. 14, č. 3. Dostupné z https://www.systemonline.cz/it-security/rozhovor-vladimir-rohel-narodni-centrum-kyberneticke-bezpecnosti.htm?mobilelayout=false

Doucek, Petr – Konečný, Martin – Novák, Luděk (2019): Řízení kybernetické bezpečnosti a bezpečnostních informací. Praha: Professional Publishing.

Drmola, Jakub (2012): Terminologie politicky motivovaných elektronických útoků a hacktivismu (seminární práce do předmětu BSS 412). Brno: Fakulta sociálních studií Masarykovy univerzity (archiv autora, citováno se svolením J. Drmoly).

Drmola, Jakub (2013): Konceptualizace kyberterorismu. Vojenské rozhledy, roč. 22, č. 54, s. 94–102.

Evropská komise (2022): Doporučení pro rozhodnutí Rady o zmocnění k jednání o komplexní mezinárodní úmluvě o boji proti využívání informačních a komunikačních technologií pro účely trestné činnosti. Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52022PC0132&from=EN

European Union (2020b): The EU's Cybersecurity Strategy for the Digital Decade. Dostupné z https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Feix, Miroslav – Procházka, Dalibor (2017): Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. Vojenské rozhledy, roč. 26, č. 3, s. 31–50.

Foldyna, Tomáš (2022): Národní korespondent pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost. Brno: Nejvyšší státní zastupitelství. Dostupné z https://verejnazaloba.cz/wp-content/uploads/2022/07/Zprava-NK-za-rok-2021-Foldyna.pdf

Gřivna, Tomáš – Polčák, Radim a kol. (2008): Kyberkriminalita a právo. Praha: Auditorium.

Havlík, Martin (2020): Jak daleko má svět k dosažení světového míru a proč? Vojenské rozhledy, roč. 29, č. 3. Dostupné z https://www.vojenskerozhledy.cz/kategorie-clanku/strategicke-rizeni/zacleneni-kybernetickych-sil

Jacobsen, Jeppe T. (2022): Cyberterrorism: Four Reasons for Its Absence – So Far. Perspectives on Terroroism, roč. 16, č. 5, s. 62–72.

Jirásek, Petr – Novák, Luděk – Požár, Josef (2015): Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, Česká pobočka AFCEA.

Kolouch, Jan (2016): CyberCrime. Praha: CZ.NIC. Dostupné z https://eknizky.sk/wp-content/uploads/2018/12/cybercrime.pdf

Kriner, Matthew – Ihler, Bjørn (2022): Analysing Terrorgram Publications: A New Digital Zine. Global Network on Extremism and Technology, https://gnet-research.org/2022/09/12/analysing-terrorgram-publications-a--new-digital-zine/

Lata, Jan (2022): Zpráva o činnosti národního koresponden-ta pro boj proti terorismu, extremismu a trestným činům spáchaným z nenávisti za rok 2021. Brno: Nejvyšší státní zastupitelství. Dostupné z https://verejnazaloba.cz/wp-content/uploads/2022/07/Zpráva-NK-za-rok--2021-Lata-.pdf

Mareš, Miroslav (2021a): Die Bekämpfung von Cyberbedro-hungen in der Tschechischen Republik. Kriminalistik. roč. 75, č. 3, s. 150–153.

Mareš, Miroslav (2021b): Vybrané sociální aspekty kyberne-tické bezpečnosti. Ostrava: Klubový večer ISACA (archiv autora).

Mareš, Miroslav – Bjørgo, Tore (2019): Vigilantism against migrants and minorities: Concepts and goals of current research. In Edited by Bjørgo, Tore – Mareš, Miroslav (eds.): Vigilantism against Migrants and Minorities. London: Routledge, Taylor & Francis, s. 1–30.

Mareš, Miroslav – Novák, Daniel (2019): Ústavní zákon o bezpečnosti České republiky. Komentář. Praha: Wol-ters Kluwer.

Mareš, Miroslav – Výborný, Štěpán (2015): Foreign fighters z pohledu českého trestního práva. The Science for Population Protection, roč. 7, č. 2, s. 1–11.

Mareš, Miroslav – Suchánek, Marek (2015): Reform of the Police of the Czech Republic: An unfinished business? Central European Papers, roč. 3, č. 1, s. 78–98.

Ministerstvo obrany České republiky (2017): Obranná strate-gie. Dostupné z https://www.vlada.cz/assets/ppov/brs/dokumenty/obranna-strategie-2017.pdf

Ministerstvo obrany České republiky (2021): Národní strate-gie čelení proti hybridnímu působení. Dostupné z https://mocr.army.cz/assets/informacni-servis/zpravo-dajstvi/narodni-strategie-pro-celeni-hybridnimu-puso-beni.pdf

Ministerstvo pro místní rozvoj České republiky (2019): Meto-dika a manuál pro práci s Databází strategií. Dostupné z https://www.dataplan.info/texty/Metodika-a-manual--Databaze-strategii-2019_v190731.pdf

Ministerstvo pro místní rozvoj České republiky (2022): Databáze strategií. Dostupné z https://www.databaze--strategie.cz

Národní centrála proti organizovanému zločinu (2022): Výroč-ní zpráva NCOZ. Praha: Národní centrála proti organizo-vanému zločinu Služby kriminální policie a vyšetřování. Dostupné z https://www.policie.cz/clanek/vyhodnoceni--cinnosti-vyrocni-zprava-ncoz-2021.aspx

Národní úřad pro kybernetickou a informační bezpečnost (2021): Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025, https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni--plan/

Národní úřad pro kybernetickou a informační bezpečnost (2022a): Strategie/Akční plán. Dostupné z https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

Národní úřad pro kybernetickou a informační bezpečnost (2022b): Vládní CERT. Dostupné z https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

Národní úřad pro kybernetickou a informační bezpečnost (2022c): Upozornění na zvýšené riziko DDOS útoků proti českým subjektům v kontextu geopolitické situace a incidentů proběhlých v posledním měsíci. Dostupné z https://www.nukib.cz/download/aktuality/221101_upo-zornn%20na%20riziko%20DDoS%20tok.pdf

Nejvyšší soud České republiky (2021): 3 Tdo 1287/2020-2992. ECLI:CZ:NS:2021:3.TDO.1287.2020.1. Dostupné z https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/81D2D452ABA65F51C12586D00018759F?openDocument&Highlight=0,null,sýrie

Nejvyšší soud České republiky (2022): 4 Tdo 192/2022-1121. ECLI:CZ:NS:2022:4.TDO.192.2022.1. Dostupné z https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSear-ch/1B7D1F610A4EC59AC12588A60017E99F?openDocu-ment&Highlight=0,null,teristického,útoku

North Atlantic Treaty Organisation (2022a): AAP-06. Slovník NATO s termíny a definicemi (anglicky a francouzsky). Praha: Úřadem pro obrannou standardizaci, katalogizaci a státní ověřování jakosti. Odbor obranné standardizace. Dostupné z https://oos.army.cz/sites/oos.army.cz/files/dokumenty/zakladni-stranka/aap-062020_cze.pdf

North Atlantic Treaty Organisation (2022b): Startegic Con-cept 2022. Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022. Dostupné z https://www.nato.int/strategic-concept/

Pačka, Roman (2019): CSIRT: v přední linii boje proti kybernetickým hrozbám. Brno: Centrum pro studium demokracie a kultury.

Pačka, Roman – Mareš, Miroslav (2022): Achieving Cyber Power Through Integrated Government Capability: Factors Jeopardizing Civil-Military Cooperation on Cyber Defense. Journal of Applied Security Research (online first). Dostupné z https://www.tandfonline.com/doi/abs/10.1080/19361610.2021.2006033?journalCode=-wasr20

Pokyn policejního prezidenta č. 103/2013 ze dne 28. květ-na 2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení, v platném znění. Dostupné z https://www.trestonline.cz/legisla-tiva/pokyn-policejniho-prezidenta/

Polčák, Radim – Harašta, Jakub – Stupka, Václav (2016): Právní problémy kybernetické bezpečnosti. Brno: Masa-rykova univerzita, Právnická fakulta.

Policie ČR (2021): Vishing a spoofing. Dostupné z https://www.policie.cz/clanek/vishing-a-spoofing.aspx

Parlament České republiky. Poslanecká sněmovna (2021): Tisk 86/0. Vládní návrh zákona, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších

předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony. Dostupné z https://www.psp.cz/sqw/text/orig2.sqw?idd=201016

Pavlíková, Miroslava - Mareš, Miroslav (2018): Techniky robotické propagandy na sociální síti Twitter. Revue pro právo a technologie, roč. 9, č. 18, s. 21–22.

Prucková, Michaela (2021): Česko na prahu přijetí novely o Vojenském zpravodajství. Co je kybernetická obrana a kam zemi posune? Právo 21. Dostupné z https://pravo21.cz/pravo/cesko-na-prahu-prijeti-novely-o-vojenskem-zpravodajstvi-co-je-kyberneticka-obrana-a-kam-zemi-posune

Psychogiou, Vasiliki (2022): Cyberspace: Is NATO doing enough? Brussels: Finabel European Army Interoperability Centre. Dostupné z https://finabel.org/cyberspace-is-nato-doing-enough/

Rada Evropské unie (2022): Rada se dohodla na posílení bezpečnosti dodavatelských řetězců IKT. Dostupné z https://www.consilium.europa.eu/cs/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/

Richterová, Anna (2021): Zahraniční bojovníci a možnosti jejich trestněprávního postihu. Praha: Univerzita Karlova. Právnická fakulta.

Riethofová, Alžběta (2018): Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR. Ministerstvo obrany. Dostupné z https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kybernetic-ke-obrany-cr-201906/

Síť revolučních buněk (2018): Na Rise-Up je policejní internacionála krátká (stažená stránka v archivu autora).

Smejkal, Vladimír (2022): Kybernetická kriminalita. 3. vydání. Plzeň: Aleš Čeněk.

Ullah, Haroon K. (2017): Digital World War. Islamists, Extremists, and the Fight for Cyber Supremacy. New Heaven and London: Yale University Press.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (nedat.): Structure of the comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Dostupné z https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/Convention_Structure.pdf

United Nations Office on Drugs and Crime (2022): Meetings of the Ad Hoc Committee. Dostupné z https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Vaca, Jan (2022): Tomáš Kubík (Policie ČR): Platům v soukromé IT sféře nemůžeme konkurovat, proto hledáme srdcaře. Lupa. Dostupné z https://www.lupa.cz/clanky/tomas-kubik-policie-cr-platum-v-soukrome-it-sfere-nemuzeme-konkurovat-proto-hledame-srdcare/

Vláda České republiky (2016): Audit národní bezpečnosti. Praha: MVČR.

Vláda České republiky (2021): Statut Výboru pro kybernetickou bezpečnost. Dostupné z https://www.vlada.cz/assets/ppov/brs/pracovni-vybory/Kyberneticka_bezpecnost/statut-vkb.pdf

Vláda České republiky (2022): Programové prohlášení vlády České republiky. Dostupné z https://www.vlada.cz/cz/programove-prohlaseni-vlady-193547/

Zákon č. 141/1961 Sb., o trestním řízení soudním, v platném znění.

Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, v platném znění.

Zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), v platném znění.

Zákon č. 40/2009 Sb., trestní zákoník, v platném znění.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

Zákon č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony.

Završník, Aleš (2017): Kyberkriminalita. Praha: Wolters Kluwer.

NOTES

newdirection.online @europeanreform @europeanreform NDeuropeanreform contact@europeanreform.org