POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra veřejnoprávních disciplín

Zajišťování obrany České republiky v kybernetickém prostoru

Diplomová práce

Ensuring the defense of the Czech Republic in cyberspace

Diploma thesis

VEDOUCÍ PRÁCE

doc. JUDr. Jan Kudrna, Ph.D.

AUTOR PRÁCE

Mgr. Bc. Michal Daněk

PRAHA

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 13. 3. 2023

Mgr. Bc. Michal Daněk

PODĚKOVÁNÍ

Tímto by autor práce rád poděkoval panu doc. JUDr. Janu Kudrnovi, Ph.D., za odborné vedení a dobrou zpětnou vazbu během tvorby této diplomové práce.

ANOTACE

Práce pojednává o zajišťování obrany České republiky v kybernetickém prostoru zejména z institucionálního hlediska. V první kapitole autor práce definuje základní terminologii. V druhé kapitole pojednává v širším pojetí o nástrojích České republiky, které významnou měrou přispívají k zajišťování bezpečnostních zájmů České republiky v kybernetickém prostoru. Třetí kapitolu vyčleňuje Vojenskému zpravodajství, které je pro toto téma významné. V kapitole čtvrté se práce věnuje mezinárodní komparaci, jelikož jsou pro kyberprostor státní hranice irelevantní. V kapitole páté pak autor práce představuje návrhy zefektivnění zajišťování kybernetické bezpečnosti České republiky. Významným způsobem se práce věnuje nedostatkům České republiky v této oblasti a navrhuje možnosti řešení.

KLÍČOVÁ SLOVA

kybernetická bezpečnost * NÚKIB * kybernetická kriminalita * metaverse * Vojenské zpravodajství * Digitální a informační agentura * jednotná doména .gov.cz

ANNOTATION

The thesis deals with ensuring the defense of the Czech Republic in cyberspace, especially from an institutional point of view. In the first chapter, the author defines the basic terminology. The second chapter is focused on tools of the Czech Republic, which ensure the security interests of the Czech Republic in cyberspace. In the third chapter, the work is devoted to Military Intelligence of the Czech Republic. The Fourth chapter deals with international comparison, since for cyberspace the state borders are de facto irrelevant. In the fifth chapter, the author of the thesis presents proposals for streamlining the cyber security of the Czech Republic. In a significant way, the work deals with the shortcomings of the Czech Republic's possibilities and suggests possible solutions.

KEYWORDS

cyber security * NÚKIB * cyber crime * metaverse * Military intelligence * Digital and information agency * unified domain .gov.cz

Obsah

Úvod

Téma diplomové práce si autor zvolil především z důvodu jeho dlouhodobého zájmu o aktuální geopolitické, právní, postmoderní a futuristické záležitosti. Jednou z futuristických záležitostí je právě kybernetický prostor, jeho fungování a umění v něm přežít. Dalším důvodem je pak jeho práce právníka a projekt manažera digitalizačních projektů státu zaměřených zejména na zvýšení kybernetické bezpečnosti a UX/UI v oblasti eGovernmentu v Odboru kabinetu místopředsedy vlády pro digitalizaci na Úřadu vlády České republiky. Během řízení a koordinace některých digitalizačních projektů přichází autor práce velmi často do kontaktu se zaměstnanci NÚKIB, s budoucími zaměstnanci DIA a se zaměstnanci některých bezpečnostních organizací ČR. Z tohoto důvodu bude analytická část práce vycházet především z pracovních zkušeností a získaných znalostí během práce na některých digitalizačních projektech státní správy.

21. století je stoletím informačním, konektivity a internetu. Informace v současné době jsou již považovány za intelektuální, fixní kapitál, který neustále nabývá na hodnotě. V této souvislosti lze sledovat v posledních několika letech stále častější zájem o témata spojená se zajišťováním informační bezpečnosti, jak v soukromém, tak ve veřejném sektoru. Především pak v kyberprostoru, kam se nyní ve velkém přesouvá kriminalita, jak vyplývá z oficiálních statistik a článků zveřejněných na webových stránkách Ministerstva vnitra České republiky.[1]

„Zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana života, zdraví a majetkových hodnot je základní povinností státu.“[2] Touto základní povinností je vázána Česká republika na ústavní úrovni dle ústavního zákon č. 110/1998 Sb., o bezpečnosti České republiky (dále jen „ÚZB“).

Vedle ústředního tématu zajišťování kybernetické bezpečnosti státu se tato práce vzhledem k souvisejícím tématům bude věnovat i některým velmi aktuálním

[1] Vzrůstající kriminalita v kyberprostoru. In mvcr.cz, 2020. [online]. [cit. 2022-11-05]. Dostupné z: https://www.mvcr.cz/clanek/pozor-na-kyberprostor-ministerstvo-vnitra-podporilo-prevenci-proti-kyberkriminalite-ve-videospotech-i-v-brozure.aspx

[2] Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. Čl. 1.

záležitostem jako je například vznik nové Digitální a informační agentury a záměr migrace na jednotnou doménu *.gov.cz.

Jako zdroj informací pro tuto práci bude použita především odborná literatura v elektronické podobě, odborné články, aktuální statistiky, oficiální weby tuzemských i zahraničních státních institucí a jejich příspěvky a komentáře, přednášky a stanoviska tuzemských i zahraničních státních představitelů. Cenné informace bude autor práce čerpat i ze svých znalostí a pracovních zkušeností získaných na Právnické fakultě Univerzitě Karlovy, při současném studiu na Policejní akademii České republiky a při současné práci v Odboru kabinetu místopředsedy vlády pro digitalizaci na Úřadě vlády České republiky.

Vzhledem k tématu této diplomové práce bude autor pracovat především s aktuálními elektronickými zdroji, jelikož autor práce shledává jemu známé knižní zdroje pojednávající o kybernetickém prostoru buď zastaralé, nebo s již neúplnými informacemi.

1. Terminologie v oblasti kybernetické obrany a bezpečnosti

Autor práce si dovolí začít v první kapitole přiblížením nebo definováním některých pojmů, které se v oblasti obrany a bezpečnosti kybernetickém prostoru často užívají a s kterými bude pracovat i tato diplomová práce.

1.1. Kybernetický prostor

Kyberprostor je jinými slovy virtuální, nehmotný prostor, který nemá začátek ani konec a není tedy ohraničený. Lze jej definovat obecně jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*[3], kteroužto definici lze nalézt v zákoně o kybernetické bezpečnosti.

Kořen slova tohoto pojmu „kyber“ je převzatý s anglického „cyber“. Poprvé byl tento termín „cyberspace“ použit Williamem Gibsonem roku 1984 v knize Neuromancer. V této knize Cyberspace také definoval jako:

„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v prostoru mysli, klastry a konstelace dat." [4]

Dalo by se nalézt spousty dalších definicí, mezi mezinárodně uznávanou definici lze například ještě zmínit tuto:

„*Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery, atd..), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení*

[3] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), § 2 písm. a).
[4] GIBSON William, Neuromancer, Laser-books, 2010, ISBN 978-80-7193-318-2.

počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“[5]

Jinými slovy a stručně řečeno je to virtuální svět tvořící globální počítačovou síť, která je základem online komunikace a výměny naprosté většiny dat ve vyspělých zemích.

Kybernetický prostor a moderní informační technologie jsou součástí života občanů téměř všech vyspělých demokratických právních státech, kvůli tomu, že ve značné míře přispívá k blahobytu společnosti. Je využíván také mimo jiné užíván díky své eminentní charakteristické vlastnosti téměř nemožné kontroly celé sítě, díky čemuž ji lze užívat teoreticky neomezenými možnostmi, a to nejen pro komunikaci a výměnu dat, ale také i pro vytváření uměleckých děl, hraní širokého spektra počítačových her, modelování virtuálních světů atp.

Pro úplnost lze zmínit, že jednou z možností nastavení distribuovaných sítí je řazení dat do šifrovaných blokových řetězců, tedy do tzv. blockchainu, který může být zcela nebo z části decentralizovanou kybernetickou sítí.

1.2. Obrana a bezpečnost

Obranou se rozumí dle právního řádu ČR *“souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému”.*[6]

Bezpečností se rozumí naproti tomu *„Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.“*[7]

---

[5] Politics in the Digital Age. In academia.edu. [online]. [cit. 2023-11-29]. Dostupné z: https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age

[6] Zákon č. 222/1999 Sb., o zajišťování obrany České republiky. § 2 odst. 1.

[7] Terminologický slovník Ministerstva vnitra ČR. [online]. 2016 [cit. 2023-02-05]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

Stručně řečeno jinými slovy, bezpečnost je žádoucí stav, obrana je opatření k zachování míry stability systému (zachování žádoucí stavu, tedy stavu bezpečnosti).

1.3. Kybernetická bezpečnost a obrana v kybernetickém prostoru

Termín kybernetická bezpečnost není definován v žádném právním předpise ČR. V prostředí tuzemska i v zahraničí lze vyhledat spousty definicí, autorovy připadá dobrá tato stručná definice: *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“.*[8]

S kybernetickou bezpečností lze nicméně spojit další záležitosti a rozdělit prostředky směřující k zajišťování žádoucího stavu akceptovatelné míry kybernetické bezpečnosti.

Zajišťování kybernetické bezpečnosti lze ještě dále dělit na proaktivní přístup, tedy hrozbám předcházející, a reaktivní přístup, tedy na hrozby nebo incidenty reagující.

Proaktivní kybernetická opatření lze definovat takto:

“Proaktivní opatření za účelem detekce či získání informace o kybernetickém průniku, kybernetickém útoku nebo hrozící kybernetické operaci, nebo pro určení původu operace, které v sobě zahrnuje spuštění útočně preventivní, preventivní nebo kontra-operace proti zdroji.”[9]

Zachovávání kybernetické bezpečnosti (tedy žádoucího stavu) a obrana České republiky v kybernetickém prostoru (tedy přijímání konkrétních opatření, ať již preventivních nebo reaktivních) jsou dvě množiny, které se dle našeho názoru autora této práce z části překrývají.

Do souhrnu opatření přijímaných v rámci *“obrany ČR v kybernetickém prostoru”* lze přiřadit i mnoho opatření přijímaných v rámci zajišťování a zachování *“kybernetické bezpečnosti”* a naopak. V případě kybernetického útoku totiž často

[8] Terminologický slovník Ministerstva vnitra ČR. [online]. 2016 [cit. 2023-02-05]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx
[9] Terminologický slovník Ministerstva vnitra ČR. [online]. 2016 [cit. 2023-02-05]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

nelze, a to mnohdy ani ex post, rozpoznat, jestli jde o útok soukromoprávního subjektu jednotlivce přicházející z tuzemska nebo o aktéra politicky významného ze zahraničí.

NÚKIB má ve své působnosti chránit (v rámci své agendy kybernetické bezpečnosti) kybernetickou infrastrukturu téměř všech orgánů veřejné moci, kteréžto orgány státní moci tvoří společně integrální součást České republiky jako celek. Kybernetická bezpečnost všech orgánů veřejné moci je dle aktuálních koncepčních dokumentů významným strategickým bezpečnostním zájmem České republiky[10] a také eminentní součástí efektivní a akceschopné obrany České republiky. Jelikož se tedy obě sféry bezpečnosti a obrany překrývají a doplňují, nelze je dle názoru autora této práce oddělit a jasně stanovit jejich hranice.

Podrobněji o institucionálních nástrojích státu v oblasti kybernetické bezpečnosti bude dále autor této práce pojednávat v kapitole druhé této diplomové práce.

1.4. Kyberterorismus

Mezi odborníky je kyberterorismus chápán jako podmnožina terorismu.[11] Uznávanou definicí kyberterorismu je většinou politicky nebo nábožensky motivovaného útoku organizovaných skupin, jednotlivců nebo příslušníků bezpečnostních sborů namířený proti jakékoliv elektronizované záležitosti zpravidla v prostředí digitálních dat, informačních sítích nebo počítačových programů.[12] Lze nabídnout i definici Dorothy Denningové:

"Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit

[10] Bezpečnostní strategie České republiky z roku 2015, kapitola III., bezpečnostní zájmy.
[11] DRMOLA, Jakub. Konceptualizace kyberterorismu. Vojenské rozhledy. 2013, č. 2.
[12] COLARIK, Andrew M. a Lech JANCZEWSKI. Managerial Guide for Handling Cyber-terrorism and Information Warfare [online]. 2005 [cit. 2015-02-08]. Dostupné z: http://www.google.cz/books?hl=cs&lr=&id=h2WJFjVhDnYC&oi=fnd&pg=PR8&dq=Janczewski+a+Colarik+2005&ots=FfUVoB9nu1&sig=-X2rajxXlpe9HhGw9QkqT0PyxAs&redir_esc=y#v=onepage&q=Janczewski%20a%20Colarik%202005&f=false

nebo donutit vlády, nebo obyvatele k podporování sociálních nebo politických cílů"[13]

Kybernetický prostor je využíván i pro záškodné a ničivé aktivity nepřátelských stran zejména díky jeho decentralizovanosti a téměž nemožné kontroly či uzurpování si internetové sítě jen pro potřebu určité velmoci. Aby kyberterorismus naplnil výše uvedené definice, měl by skutečně faktický výrazně negativní dopad na cílovou skupinu obyvatel. Negativní dopad lze chápat v podobě ohrožení či faktickému poškození bezpečnostních zájmů cílové skupiny obyvatel či samotného systému státu či určité jiné soukromoprávní struktury. Toto ohrožování či poškozování zájmů může nabývat různou podobu přes psychické vyhrožování, narušení toku informací, mazání dat, vyřazení elektronických zařízení z provozu, šíření strachu, nejistoty či jiných negativních emocí po faktickou destrukci určitého systému.

Někteří autoři jsou toho názoru, že primární cíl terorismu i kyberterorismu je změna chování nebo politiky cílové skupiny obyvatel zpravidla prostřednictvím manipulace nebo šíření či vyvolávání strachu, nebo prostřednictvím propagandy a právě se hodicím ideálů nebo skrz oslabení majetkových či finančních poměrů protivníka. Primární cíle kyberterorismu jsou tedy zpravidla v reálném, fyzickém světě, přestože se jejich velká část odehrává ve světě nehmotném, na kterém je moderní společnost čím dál více závislá. Dle většiny názorů je tedy hlavním objektem kyberterorismu lidská psychika.

1.5. Kyberkriminalita

Kyberkriminalita je trestná činnost páchána v prostředí internetových sítí a v širší pojetí v celém spektru oblasti informačních technologií nebo prostředky informačních či komunikačních technologií.[14]

[13] DENNING, Dorothy E. Activism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In iwar.org.uk [online]. [cit. 2023-03-10]. Dostupné z: http://www.iwar.org.uk/cyberterror/resources/denning.htm Archivováno

[14] Prevence kriminality. In prevencekriminality.cz [online]. [cit. 2023-01-30]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

Kyberkriminalita jako jedna z mála oblastí páchání trestných činů v podstatě od prvního výskytu užívání internetu na území ČR v podstatě neustále stoupá. V posledních letech dokonce téměř exponenciálně.[15]

Tato práce se zabývá tímto pojmem především z toho důvodu, že podobně jako u obrany a bezpečnosti mezi kyberútoky spáchanými subjekty soukromého práva a veřejného práva není zřetelný rozdíl a často u značného množství latentních trestné činů nelze ani ex post zjistit zdroj útoku.

Kyberkriminalitu lze dělit na sofistikovanou a běžnou.

Mezi nejvýznamnější druhy kyberkriminality (které lze nicméně páchat i subjekty mezinárodního práva, včetně států) lze zařadit:

- Podvod dle § 209 zákona č. 40/2009 Sb., trestního zákoníku - lze pod touto skutkovou podstatu zařadit "reverzní inzertní podvody" - vylákání údajů o platební kartě, tzv. "blagging" (podvodná žádost o finanční pomoc nebo tzv. "neočekávané peníze" - údajně získané dědictví, loterie, zaslání 5 bitcoinu atp.)[16], podvodné telefonáty a "podvodné e-shopy" (podvodníci vydávající se za solidního podnikatele nebo prodávajícího) nebo například podvody s láskou (milostným příběhem) "Americký voják".
- Hacking, pod který lze zařadit ve většině případů neoprávněný přístup k počítačovému systému a nosiči informaci dle § 230 trestního zákoníku a trestný čin porušení tajemství dopravovaných zpráv dle § 182 trestního zákoníku.

  Zde bych upozornil na významně aktuální a mimořádně nebezpečnou záležitost tzv. "ukládání hesel do prohlížeče Chrome". V rámci velké důvěry, které do ukládání hesel občané vkládají, by se mohl v případě úspěšného útoku aktér mohl dostat teoreticky ke všem osobním údajům a

[15] Konference Den bezpečnější internetu 2023. In youtube.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://www.youtube.com/watch?v=DawSAQSLBrc
[16] Podvody s kryptoměnami. In finex.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://finex.cz/nejcastejsi-podvody-s-bitcoinem-na-toto-si-dejte-pozor/

bankovním účtům případně poškozeného. Na tuto záležitost opakovaně upozorňuje NÚKIB i Národní centrála proti organizovanému zločinu.[17]

- Sexuální trestné činy spojené s šířením pornografie, ať už dětské nebo dle § 191 nebo dle § 193, § 193a nebo § 193b trestního zákoníku nebo přes internet páchané trestné činy spojené s lidskou důstojností jako například obchodování s lidmi dle § 168 trestního zákoníku.
- Hate crimes, v češtině nebezpečné projevy nenávisti, zejména na sociálních sítích, do kteréžto skupiny lze zařadit vydírání dle § 175 trestního zákoníku, dále *stalking*, v češtině trestný čin nebezpečné pronásledování dle § 354 a nebezpečné vyhrožování dle § 353 trestního zákoníku a například hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355 trestního zákoníku.

[17] Konference Den bezpečnější internetu 2023. In youtube.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://www.youtube.com/watch?v=DawSAQSLBrc

2. Nástroje České republiky při obraně v kyberprostoru

Jak již v úvodu této diplomové práce autor práce předeslal, zajišťování bezpečnostních zájmů ČR je základní povinností státu.[18]Ze všech složek státní moci je to složka výkonná, která má na starosti zajišťování obrany a bezpečnosti ČR. Zajišťování bezpečnostních zájmů České republiky a řízení a funkčnost bezpečnostního systému ČR je odpovědná jako vrcholný orgán výkonné moci[19] vláda.

Vláda sama jako vrcholný orgán výkonné moci vzhledem k rozsahu působnosti nemůže řešit všechny odborné a specifické záležitosti sama, tudíž například pro efektivní zajišťování kybernetické bezpečnosti a koordinaci orgánů státní správy bylo zřízeno několik státních institucí, o kterých bude autor této práce psát dále v této kapitole a v kapitole třetí.

Autor práce si dovoluje rozdělit nástroje rozdělit z hlediska úrovně aplikace na:

1) Centrální neboli strategickou úroveň
2) Taktickou úroveň
3) Operativní úroveň

Dále si autor práce dovoluje rozdělit nástroje pro zajišťování kybernetické bezpečnosti na:

1) Koncepční nástroje
2) Institucionální nástroje
3) Zdrojové nástroje

2.1. Koncepční nástroje

V zájmu zachování přehledného členění této práce se rozhodl autor práce rozdělit koncepční nástroje na legislativní a nelegislativní materiály.

2.1.1. Legislativní materiály

Z hlediska kybernetické bezpečnosti je jedním z nejvýznamnějších aktuálně účinných zákonů zákon č. 181/2014 Sb., o kybernetické bezpečnosti, s účinností

[18] Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. Čl. 1.
[19] Ústavní zákon č. 1/1993 Sb., Ústava České republiky. Čl. 67 odst. 1.

od 1. ledna 2015 a na úrovni podzákonných právních předpisů jeho prováděcí vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, známá jako vyhláška o kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti upravuje působnost a kompetencí některých institucionálních nástrojů ČR (působnost NÚKIB, národního CERT a vládního CERT), o který bude pojednáno v dalších podkapitolách, zapracovává příslušné předpisy Evropské unie (které zpracovávají také novely[20] tohoto zákona), ale především upravuje práva a povinnosti osob v oblasti kybernetické bezpečnosti.[21] V tomto ohledu je převážně ve vztahu speciality k obecnější úpravě tzv. digitální ústavě[22] a některým dalším zákonům upravující problematiku eGovernmentu.[23]

Mezi hlavní cíle tohoto zákona patří:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty a
- upravit činnost dohledových pracovišť[24].

Vyhláška o kybernetické bezpečnosti dle svého aktuálního znění upravuje:

> ***"a)*** *obsah a strukturu bezpečnostní dokumentace,*
>
> ***b)*** *obsah a rozsah bezpečnostních opatření,*

[20] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění zákona č. 104/2014 Sb., a některé další zákony.
[21] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. § 1 odst. 1.
[22] Zákon č. 12/2020 Sb., o právu na digitální služby (digitální ústava).
[23] například zákon č. 111/2009 Sb., o základních registrech nebo zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
[24] Legislativa kybernetické bezpečnosti. In nukib.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

c) *typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,*

d) *náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,*

e) *náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,*

f) *vzor oznámení kontaktních údajů a jeho formu a*

g) *způsob likvidace dat, provozních údajů, informací a jejich kopií."*[25]

Pro obranu České republiky v kybernetickém prostoru patří mezi nejvýznamnější zákony zákon č. 289/2005 Sb., o Vojenském zpravodajství, který díky nedávné novelizaci zákonem č. 150/2021 Sb. svěřil poměrně významné nástroje VZ jako vojenské rozvědné i kontrarozvědné zpravodajské službě v oblasti obrany v kybernetickém prostoru. O těchto nástrojích, kompetencích a působnosti VZ bude dále pojednáno v dalších kapitolách této práce.

Jako další právní předpisy relevantní z hlediska kybernetické bezpečnosti (například z důvodu digitalizace, elektronizace nebo výstavby informační sítích veřejné správy) nebo s touto tématiku související lze zmínit:

- tzv. Směrnice NIS, celým názvem Směrnice Evropského parlamentu a Rady Evropské unie č. 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.[26] Tato směrnice sleduje harmonizaci právní úpravu členských států EU v oblasti bezpečnosti internetových sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti členských států EU. Směrnice NIS mimo jiné rozšiřuje okruh provozovatelů základní služby a poskytovatele digitálních služeb (cloud computing, internetové vyhledávače, NFT marketplaces, poskytovatelé online her či virtuálních realit), pro které budou stanoveny povinnosti v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty. Požadavky směrnice

[25] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, známá jako vyhláška o kybernetické bezpečnosti. § 1 písm. a) až g).
[26] Směrnice Evropského parlamentu a Rady Evropské unie č. 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

zapracovává novela zákona o kybernetické bezpečnosti cestou zákona č. 205/2017 Sb. s účinností od 1. srpna 2017 (viz příslušná sekce stránek NÚKIB).

V této souvislosti považuje autor práce ještě vhodné zmínit, že NÚKIB aktuálně připravuje ve spolupráci s ostatními orgány státní správy a odbornou veřejností znění nového zákona o kybernetické bezpečnosti, který po prvotních konzultacích ze strany odborné veřejnosti půjde tento rok do meziresortního připomínkového řízení.[27]

- zákon č. 240/2000 Sb., o krizovém řízení, známý jako krizový zákon, který upravuje postup IZS, orgánů krizového řízení a dalších ze zákona povinných osob v případě vyhlášení jedním z krizových řízení.
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která má za cíl určit významné informační systémy veřejné správy a určení jejich kritérií.
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury ČR, přičemž je vymezeno konkrétně 9 odvětví.
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.
- A dále pak vyhlášky upravující užívání cloud computing č. 315/2021 Sb., o bezpečnostních pravidlech a 316/2021 Sb., o zápisu do katalogu.

Pro úplnost považuje autor této práce vhodné zmínit sestupně dle data přijetí i tzv. zákony eGovernmentu bezprostředně související s digitalizací orgánů veřejné moci, a tím pádem i se zvyšováním kybernetické bezpečnosti:

- Zákon č. 89/1995 Sb., o státní statistické službě,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Zákon č. 111/2009 Sb., o základních registrech,

[27] Návrh nového zákona o kybernetické bezpečnosti. In osveta.nukib.cz [online]. [cit. 2023-03-10]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 250/2017 Sb., o elektronické identifikaci,
- Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací,
- Zákon č. 12/2020 Sb., o právu na digitální služby (tzv. digitální ústava).

2.1.2. Nelegislativní materiály

Vedle legislativních aktů přijímá ze strategické neboli centrální úrovně vláda i koncepční dokumenty, které však na rozdíl od legislativních aktů nejsou zpravidla žádnými právními prostředky vymáhány, pokud na ně právní předpisy přímo neodkazují.

Mezi nejvýznamnější strategické dokumenty patří:

- Národní strategie kybernetické bezpečnosti 2020-2025,
- Bezpečnostní strategie České republiky 2015, v které se zajištění kybernetické bezpečnosti a obrany ČR řadí do tzv. strategických zájmů,
- Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025,
- Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost,
- Obranná strategie České republiky z roku 2017

2.2. Institucionální nástroje

Zjednodušeně řečeno, v současné době agenda zajišťování obrany v kybernetickém prostoru České republiky na státní a mezinárodní úrovni v kybernetickém prostoru je svěřena Vojenskému zpravodajství a agenda zajišťování kybernetické bezpečnosti státních institucí Národnímu úřadu pro kybernetickou a informační bezpečnost. Zprostředkovaně hrají významnou roli v zajišťování kybernetické bezpečnosti i vybraný provozovatel národního CERT,

kterým je v současné době sdružení zájmových právnických osob CZ.NIC.[28] A tzv. vládní CERT, který je dle zákona o kybernetické bezpečnosti součástí NÚKIB.

Česká republika však disponuje i dalšími koordinačními, podpůrnými či řídícími institucionálními nástroji, ty stěžejní uvádím v podkapitolách této kapitoly druhé.

2.2.1. Zpravodajské služby České republiky

Zpravodajské služby ČR jsou státní organizace, které mají za úkol poskytovat informace zákonným adresátům o hrozbách pro bezpečnost země a tím významně přispívat k zajišťování bezpečnostních zájmů ČR. Česká republika má k dispozici v době psaní této práce 3 zpravodajské služby, jsou jimi: Bezpečnostní informační služba (zkratkou BIS), Vojenské zpravodajství (zkratkou VZ) a Úřad pro zahraniční styky a informace (zkratkou ÚZSI). Za jejich činnost je odpovědná vláda[29], která zároveň schvaluje i jejich statuty, které upravují vnitřní organizaci ZS ČR a bližší vymezení jejich činností.[30]

V kyberprostoru mají zpravodajské služby významnou úlohu. V 21. století je a bude kyberprostor důležitým místem (v zahraničí se již hovoří stále častěji o Metaverse, tedy o virtuálních světech, jako o v podstatě synonymum pro kyberprostor)[31] pro hospodářský a informační rozvoj a bezpečnost země. V tomto prostředí se stále více objevují různé bezpečnostní, ale i ekonomické hrozby pro národní bezpečnost, jakými jsou špionáž, dezinformační kampaně a mnohé příklady kyberkriminality popsané v kapitole 1.5. Zpravodajské služby se proto zaměřují na monitorování kyberprostoru a sledování aktivit, které mohou ohrozit bezpečnost státu.

Mezi hlavní obecné úkoly zpravodajských služeb v kyberprostoru patří sběr informací o kybernetických hrozbách, monitorování cílených útoků na státní instituce, kritickou infrastrukturu a další důležité subjekty, identifikace zdrojů kyberútoků a případné podání návrhu na protiopatření, poskytování informací o kybernetických hrozbách ostatním bezpečnostním složkám státu a spolupráce s

[28] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti České republiky.
[29] Zákon č. 153/1994 Sb., o zpravodajských službách České republiky. § 7.
[30] Zákon č. 153/1994 Sb., o zpravodajských službách České republiky. § 6.
[31] What is Metaverse? In wired.com [online]. [cit. 2023-02-15]. Dostupné z: https://www.wired.com/story/what-is-the-metaverse/

mezinárodními partnery v oblasti kybernetické bezpečnosti, jak vyplývá z § 5 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.[32]

Jak uvádí mezi českými zpravodajskými službami veřejnosti nejznámější, Bezpečnostní informační služba, BIS spolupracuje s více než stovkou jiných ZS s více než 65 zemí.[33] Z toho lze implicitně vyvodit, že BIS udržuje vzájemný kontakt i se zeměmi mimo NATO, jelikož počet členských států NATO je v době psaní této diplomové práce 30. V době psaní této diplomové práce nicméně probíhají poměrně intenzivní jednání ohledně případného vstupu Švédska a Finska do NATO[34]. Všechny členské země již vyjádřily písemný souhlas s tím rozšířením kromě Turecka a Maďarska. O vstup do NATO usiluje rovněž dlouhodobě Ukrajina. V tomto případě se nicméně proces vstupu vzhledem ke geopolitickým a vnitropolitickým podmínkám Ukrajiny zatím ani nepřibližuje aktuálnímu postupu Švédska a Finska. A to přestože členství bylo Ukrajině a Gruzii přislíbeno v roce 2008 na summitu NATO v Bukurešti.[35]

Zpravodajské služby ČR jsou také zodpovědné za poskytování informací a poskytování doporučení v oblasti kybernetické bezpečnosti především vládě. Zpravodajské služby ČR by však měly vhodně formulované zpravodajské informace předávat vhodným způsobem i dalším prvkům bezpečnostního systému České republiky, například NÚKIB, NBÚ, ozbrojeným složkám nebo bezpečnostním sborům ČR, s kterými by zpravodajské služby ČR měly v co nejvyšší možné míře spolupracovat.[36] Vysoká míra vzájemné spolupráce by samozřejmě měla fungovat i mezi zpravodajskými službami samotnými, a to včetně spojeneckých zpravodajských služeb členských států NATO a Evropské unie. Poskytované zpravodajské informace jsou především pro vládu důležité pro

[32] Zákon č. 153/1994 Sb., o zpravodajských službách České republiky. § 5.
[33] Mezinárodní kontakty BIS. In bis.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.bis.cz/mezinarodni-spoluprace/
[34] NATO, list of countries which agreed with Finland and Sweden accession to NATO. In nato-pa.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato-pa.int/content/finland-sweden-accession
[35] NATO Bucharest Summit Declaration. In nato.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato.int/cps/en/natolive/official_texts_8443.htm
[36] Spolupráce zpravodajských služeb. In bis.cz [online]. [cit. 2023-02-16]. Dostupné z: https://www.bis.cz/mezinarodni-spoluprace/mezinarodni-spoluprace-e769e1ea.html

plánování, pro strategické rozhodování a provádění opatření k ochraně kybernetické kritické infrastruktury a k zajišťování bezpečnostních zájmů ČR.

Zpravodajské služby České republiky se musí neustále průběžně přizpůsobovat novým hrozbám a výzvám v rychle se vyvíjejícím kybernetickém prostoru. Je důležité, aby tyto služby disponovaly moderními technologiemi a dostatečnými zdroji, aby byly schopné účinně reagovat na tyto nové hrozby a výzvy. O těchto doporučeních bude více pojednáno v následujících kapitolách a v závěru této práce.

ZS ČR, zejména Vojenské zpravodajství, využívají moderní technologie a speciální software pro sběr a analýzu informací v kyberprostoru. Tyto nástroje umožňují získávat informace z různých zdrojů a v reálném čase. Součástí těchto nástrojů jsou například antivirové programy, firewally, systémy detekce útoků a systémy pro analýzu dat.

Zpravodajské služby ČR také provádějí ve spolupráci s NÚKIB vzdělávací aktivity pro veřejnost a podniky, aby zvýšily povědomí o kybernetické bezpečnosti, a pomohly tak předcházet kybernetickým útokům. Stěžejními výstupy, které bývají často zmiňovány, jsou výroční zprávy zejména BIS.[37]

Celkově lze říci, že zpravodajské služby České republiky mají v kyberprostoru důležitou úlohu. Sběr informací o kybernetických hrozbách, analýza dat a výměna informací s dalšími bezpečnostními složkami státu jsou klíčové pro ochranu kybernetické bezpečnosti a dalších bezpečnostních zájmů státu.

Autor práce považuje za důležité, aby ZS ČR byly vybaveny moderními technologiemi a dostatečnými zdroji, aby mohly účinně plnit své úkoly a přizpůsobovat se novým výzvám a hrozbám v kyberprostoru.

Ze zmíněných českých zpravodajských služeb má za úkol zajišťovat obranu v kybernetickém prostoru Vojenské zpravodajství. Této zpravodajské službě konkrétně tak z tohoto důvodu bude dále podrobněji věnována celá jedna kapitola.

[37] Výroční zpráva BIS. In bis.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/

2.2.2. Poradce pro národní bezpečnost

Vláda vytvořila dne 21. prosince 2022 usnesením č. 1078 novou funkci Poradce pro národní bezpečnost, který bude mít administrativní podporu prostředí Úřadu vlády České republiky.

Autor práce si v této podkapitole dovolí navázat na svoje dřívější teze ze své předchozí diplomové práce, kterou psal během jeho studia na Právnické fakultě Univerzity Karlovy.

Již před dvěma roky zřízení tohoto nového orgánu s předpovězeným stejným názvem předpokládal s odkazem na programové prohlášení této vlády[38] a v reakci na některé krizové záležitosti, kterými se musely bezpečnostní prvky bezpečnostního systému České republiky v posledních letech zabývat. Funkce nakonec skutečně byla zřízena po vzoru USA a Izraele.

Ta fyzická osoba by měla být vzhledem k obsahu práce kvalifikovaný bezpečnostní expert s dobrými komunikačními schopnostmi zejména v oblasti zpravodajských služeb, krizového řízení a hybridních hrozeb na celostátní a mezinárodní úrovni. Tento monokratický orgán by měl být velmi pohotový, co se informovanosti klíčovými prvky bezpečnostního systému ČR a mezi klíčovými představiteli státu bez ohledu na jejich politickou orientaci. Čelními představiteli se míní především předseda vlády, ministr vnitra, ministr obrany, ministr zahraničních věcí, ředitelé ZS ČR a například i ředitele NÚKIB.[39]

Poradce pro národní bezpečnost by měl sehrát svou roli zvýšením úrovně koordinace bezpečnostních složek během zvládání krizových situací na celostátní úrovni. Krizové situace, při kterých byla v minulosti koordinace bezpečnostních prvků bezpečnostního systému ČR vysoce potřebná, lze jmenovat např. epidemie Covid-19, během které nouzový stav[40] trval, a opakovaně se prodlužoval, pro

[38] Programové prohlášení a poradce pro národní bezpečnost. In ceskenoviny.cz [online]. [cit. 2023-01-16]. Dostupné z: https://www.vlada.cz/cz/programove-prohlaseni-vlady-193547/

[39] Superúředník pro národní bezpečnost, krizový manažer a poradce v jednom. In natoaktual.cz. [online]. [cit. 2023-01-20]. Dostupné z: https://www.natoaktual.cz/zpravy/poradce-bezpecnost-obrana-vnitro-armada-namestek-koordinator.A210722_144606_na_zpravy_m00

[40] Nouzový stav při epidemii Covid-19. In covid.gov.cz. [online]. [cit. 2022-01-20]. Dostupné z: https://covid.gov.cz/situace/onemocneni-obecne-o-opatrenich/nouzovy-stav

území celé České republiky nejdéle v historii samostatné České republiky[41], anebo mimořádná událost výbuchu ve Vrběticích a následně přijatá opatření v souvislosti s vyšetřováním v roce 2021.[42]

Vláda jmenovala usnesením vlády č. 1103 s účinností od 1. ledna 2023 Poradcem pro národní bezpečnost Tomáše Pojara, MA. Tímto usnesením se vláda také usnesla na povinnosti tohoto monokratického orgánu postupovat v souladu se Statutem Poradce pro národní bezpečnost schváleným usnesením vlády ze dne 21. prosince 2022 č. 1078[43], o vytvoření funkce poradce pro národní bezpečnost. Ukládá se zároveň členům vlády povinnost spolupracovat s tímto poradcem v oblasti zajišťování bezpečnostních zájmů a obrany České republiky.[44]

2.2.3. Národní úřad pro kybernetickou a informační bezpečnost

Ústředním správním úřadem[45] dle kompetenčního zákona pro oblast kybernetické bezpečnosti včetně oblasti ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je jako gestor těchto záležitostí Národní úřad pro kybernetickou a informační bezpečnost dle aktuálního znění zákona o kybernetické bezpečnosti a zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.[46]

NÚKIB vznikl 1. ledna 2017 zákonem č. 205/2017 Sb., kterým se novelizoval zákon č. 181/2014 Sb., o kybernetické bezpečnosti a zákon č. 2/1969 Sb., kompetenční zákon.[47] Jako určitou kuriozitu lze zmínit, že novelizační zákon uvádí ve svém zřizovacím ustanovení pouze “Úřad”, nikoliv celým názvem “Národní úřad pro kybernetickou a informační bezpečnost”, jak by adresáti zákonných norem mohli očekávat.

NÚKIB sídlí v Brně, v Praze nicméně má detašované pracoviště, které využívá pro prezenční schůze některých svých projektů. V době psaní této diplomové práce je

[41] Informace Úřadu vlády o vládních usnesení ohledně boje s epidemií. In vlada.cz. [online]. [cit. 2022-03-10]. Dostupné z: https://www.vlada.cz/cz/epidemie-koronaviru/dulezite-informace/vladni-usneseni-souvisejici-s-bojem-proti-epidemii---rok-2021-193536/
[42] Výroční zpráva BIS za rok 2021, 2023-01-20 dostupné z: https://www.bis.cz/vyrocni-zpravy/
[43] Usnesení vlády ze dne 21. 12. 2022 č. 1078.
[44] Usnesení vlády ze dne 21. 12. 2022 č. 1103, jmenování účinné od 1. ledna 2023.
[45] Zákon č. 2/1969 Sb., kompetenční zákon. § 2, bod 16.
[46] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.
[47] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. § 21a a dále.

ředitelem NÚKIB pan Ing. Lukáš Kintr. Před ním vedl NÚKIB generálmajor Ing. Karel Řehka a před ním Ing. Dušan Navrátil jako historicky první ředitel NÚKIB.[48]

NÚKIB se prostřednictvím svého ředitele, kterým je v době psaní této diplomové práce pan Ing. Lukáš Kintr, účastní jako externí host schůzí Bezpečnostní rady státu. Dle Statutu BRS totiž může BRS přizvat na schůze i vedoucí jiných ústředních orgánů státní správy.[49] NÚKIB také může na žádost BRS pro BRS dodat informace, analýzy či plnit úkoly uložené Bezpečnostní radou státu. Ředitel NÚKIB je také členem Výboru pro kybernetickou bezpečnost Bezpečnostní rady státu.

NÚKIB má dále například ve své působnosti:

- vydávání opatření, analýz a doporučení v oblasti prevence, vzdělávání a metodické podpory v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,
- provádí monitoring kybernetických hrozeb a rizik, mimo jiné například také skenuje všechny domény ve vlastnictví státu, kteréžto činnosti by měl významně pomoc projekt Odboru kabinetu místopředsedy vlády pro digitalizaci sjednocování státních domén pod doménu 1. a 2. řádu *.gov.cz.
- je poměrně aktivním připomínkovým místem v oblasti digitalizačních materiálů a legislativních i nelegislativních materiálů související s kybernetickou bezpečnosti,
- ukládá správní tresty za porušování povinností povinných osob dle zákona o kybernetické bezpečnosti a dle zákona o bezpečnostní způsobilosti a utajovaných informací[50], nebo
- problematiku regulované služby (PRS) globálního navigačního družicového systému Galileo, která je určena pouze pro autorizované uživatele,

Díky tomu, že přiznání pravomocí Vojenskému zpravodajství je stále ještě čerstvá záležitost a díky tomu, že například funkce inspektora pro kybernetickou obranu byla obsazena teprve před několika málo měsíci, podílí se na zajišťování

[48] Vedení NÚKIB. In nukib.cz [online]. [cit. 2023-02-09]. Dostupné z: https://nukib.cz/cs/o-nukib/vedeni-uradu/
[49] Statut Bezpečnostní rady státu. Čl. 9 odst. 2.
[50] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. § 22.

kybernetické bezpečnosti státních institucí, včetně obrany státu v kybernetickém prostoru do stále ještě rozhodující míry NÚKIB, který je stále vládním CERT České republiky.

Je to stále také NÚKIB, o kterém je slyšet v souvislosti s kybernetickou bezpečností státu v tuzemsku i v mezinárodním společenství, a je to stále NÚKIB, na kterého se občané i státní zaměstnanci obrací v souvislosti s kybernetickou bezpečností.

Z tohoto důvodu budou zmíněné a rozvedeny některé činnosti NÚKIB i v dalších kapitolách této diplomové práce.

2.2.4. Digitální a informační agentura

K datu 1. 1. 2023 nabyla účinnosti stěžejní ustanovení zákona č. 471/2022 Sb., novela zákona č. 12/2020 Sb., o právu na digitální služby (tzv. digitální ústava), zákona č. 2/1969 Sb., kompetenčního zákona a některých jiných zákonů, které zřizují Digitální a informační agenturu jako nový ústřední správní úřad.[51] Účinnosti zbylých ustanovení tohoto zákona nabydou až 1. dubna 2023.

Jako historicky první ředitel tohoto nového (v pořadí platného znění kompetenčního zákona) 19. ústředního orgánu státní správy byl jmenován na návrh místopředsedy vlády pro digitalizaci, Ivana Bartoše, vládou 18. ledna pan Ing. Martin Mesršmíd. Účinnost tohoto jmenování nabyla 1. února 2023. V době psaní této práce se ředitel nové Digitální a informační agentury tedy seznamuje se všemi záležitostmi a zaměstnanci, kteří 1. dubna 2023 přejdou z Ministerstva vnitra a některých podřízených organizaci MV ČR (např. Správa základních registrů)[52] a později případně i Národní agentura pro komunikaci a informační technologie (dále jen “NAKIT”).

Přestože legislativní proces byl poměrně důkladný a přestože se tímto zákonem zřizuje nový ústřední správní úřad, terminologií kompetenčního zákona ústřední orgán státní správy, čímž se musel mimo jiné otevřít kompetenční zákon, čehož se někteří legislativci obvykle obávají, byl termín a plán účinnosti tohoto zákona k

[51] Zákon č. 12/2020 Sb., o právu na digitální služby (tzv. digitální ústava). § 2a.
[52] Zákon č. 471/2022 Sb., o změně zákona o právu na digitální služby, kompetenčního zákona a dalších zákonů eGovernmentu, kterým se mimo jiné zřizuje Digitální a informační agentura jako nový ústřední správní úřad. Přechodná ustanovení.

1. 1. 2023 nakonec naplněn a platnosti tak nabyl tento zákon na konci prosince, kdy prezident, Miloš Zeman, zákon podepsal.

Jinými slovy navzdory velikosti projektu, navzdory mnoha obávám a pochybám mnohých participujících osob z jiných resortů a navzdory časové tísni se díky práci Odboru kabinetu místopředsedy vlády pro digitalizaci plán po legislativní stránce v podstatě bez větších problémů podařilo naplnit.

Nutnost rychlého zřízení nadresortního a účinného nástroje, který bude efektivně strategicky a nadresortně řídit digitalizaci státní správy napříč resorty je poměrné naléhavá. A to z několika důvodů.

Níže si dovoluje autor práce stručně demonstrativně zmínit ty nejzásadnější argumenty:

A. Chybí centrální koordinace, jednotné řízení digitální transformace a digitálních služeb, standardy, jednotná metodika a efektivní projektové řízení, sdílení kompetencí a potřebných odborných zkušenosti.

B. Chybí soustředění talentu a sdílení know-how, zkušeností a znalostí navenek do všech resortů a organizací.

C. Chybí prestižní, odborná a na výsledek orientovaná jednotní digitalizační organizace s jednotným cílem, vizí a posláním.[53]

D. Chybí udržitelné a plánované financování sdílených služeb (samostatná kapitola státního rozpočtu, víceleté plánování).

E. Agenda digitalizace státní správy je z povahy věci agenda nadresortní. Digitální agendy by měly být core business jedné silné nadresortní státní instituce, neměly by být “rozesety” různě po resortech, rozhodně by to neměla být jen jedna opomíjená část určitého velkého resorty zabývající se prioritně jinými problematikami.

F. Nevyhovující je stav tzv. sdílených služeb, kdy například základní registry tvořící páteř českého eGovernmentu jsou službou pro všechny správní

[53] Digitální a informační agentura. In profant.eu [online]. [cit. 2023-03-05]. Dostupné z: https://www.profant.eu/2022/dia.html

úřady, včetně úřadů samospráv, ale jsou v současné době podřízenou organizací Ministerstva vnitra a jsou financovány z jeho rozpočtové kapitoly.

G. Posuzování a schvalování informačních systémů veřejné správy odborem Hlavního architekta je omezené, často se děje až těsně před podpisem smlouvy s dodavatelem. Pozdější změny a zásahy do projektů se dějí mimo jakékoliv posouzení.

H. V současné době mají některá ministerstva podřízenou organizaci (zpravidla státní podnik), od které mohou nakupovat IT služby bez vypsání veřejné zakázky na základě tzv. in-house výjimky. To je však možné jen v rámci jednoho resortu. Toto uspořádání je nehospodárné, protože neumožňuje resortům sdílet vysoce odborné kapacity a neumožňuje uchování jedinečného know-how.[54]

I. Výdaje na IT jsou rozdrobené a není přehled o výdajích napříč veřejnou správou. Nejsou využívané možnosti případné synergie, není jak vyhodnotit efektivitu nákladů a investic. Chybí např. přehled o mandatorních, tj. povinných výdajích z uzavřených smluv.[55]

Ze všech výše demonstrativně vytyčených důvodů vzniku DIA lze implicitně vyčíst i primární obecné cíle DIA, tedy naplnit, vylepšit nebo všechny ty záležitosti, které v současné době nefungují, chybí nebo je třeba je významně aktualizovat.

Jako speciální cíle DIA lze významně napomoci digitálním projektům, které je třeba fakticky dotáhnout a implementovat do státní správy. Opět demonstrativně řečeno lze uvést:

[54] Důvodová zpráva, zejména její obecná část, k zákonu č. 471/2022 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony.
[55] Zákon č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Důvodová zpráva k tomuto zákona.

A. Vytvořit vhodné prostředí, v kterém se bude účinně naplňovat principy plynoucí z digitální ústavy, demonstrativně lze zmínit tyto principy:[56][57]

    a. Princip *“only once”*, tedy žádat po občanech data pouze jedno. Stát může činit žádat po občanech pouze ty data, které občany státu nikdy předtím neposkytl.

    b. Výše uvedený princip lze v podstatě pojmenovat i jako “obíhají data, nikoliv občané”.

    c. Vše, co lze alternativně digitalizovat, tak digitalizovat (za současné zachování možnosti využít i papírového nebo osobního vyřízení určitého práva).

    d. Nelze nikoho nutit využívat digitální služby - je to stále fakultativní možnost, přestože bude majoritně využívána. Všechny služby mohou i nadále užívat např. i senioři.

    e. Přístupnost, vnímatelnost, srozumitelnost, ovladatelnost a transparentnost dat.

B. Zavést tzv. elektronickou peněženku (e-Dokladovku) a propojit e-Dokladovku s portálem občana,

C. Významně rozšířit, zefektivnit a zvýšit uživatelskou přívětivost při práci s portálem občana,

D. Propojit portály pro adresáty veřejné správy s přehledným rozcestníkem *.gov.cz,

E. Zavést jednotnou doménu státní správy *.gov.cz a zavést jednotný vizuální styl internetových stránek a mobilních aplikací státní správy (aktualizovat designsystem.gov.cz),

F. Dále šířit povědomí o datových schránkách,

[56] Zákon č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Důvodová zpráva k tomuto zákona.

[57] Poznámka: Autor práce si dovolí poznamenat, že na důvodové zprávě k zákonu č. 471/2022 Sb., se významně podílel, zejména na její obecné části.

G. Zavést funkční sdílený datové fondy a portálové řešení státní správy,

H. Zefektivnit financování všech výše zmíněných projektů zejména prostřednictvím Národního plánu obnovy.[58]

Digitální a informační agentura je z právního a formálního hlediska nový úřad, nicméně fakticky vzniká sloučením Správy základních registrů a dvou stěžejních odborů Ministerstva vnitra, které se zabývají eGovernmentem a digitalizací státní správy. Na Ministerstvu vnitra se přesun týká tedy Odboru eGovernmentu a odboru Hlavního architekta eGovernmentu. Materiálně tak v podstatě nevzniká žádná nová budova nebo něco zcela nového na nové louce, pouze se přesouvají zaměstnanci do nového úřadu koncentrující digitální agendy, a sice s výjimkou agend týkající se kybernetické bezpečnosti.[59] Agendy týkající se kybernetické bezpečnosti a obrany státu v kybernetickém prostoru zůstane NÚKIB a zpravodajským službám, a ze zpravodajských služeb především Vojenskému zpravodajství.

Formálně jsou zaměstnanci Odboru Hlavního architekta eGovernmentu a Odboru eGovernmentu do 1. 4. 2023 stále organizačně pod Ministerstvem vnitra. 1. dubna totiž nastává účinnost zbylých ustanovení zákona č. 471/2022 Sb., o změně digitální ústavy, kompetenčního zákona a některých dalších zákonů.

Po 1. dubnu 2023 bude dle názoru autora kruciální nejen udržet kvalifikované lidské zdroje, které přešly z Ministerstva vnitra, ale i nabrat nové síly, které obsadí kompetenční centra a některé místa, která byla na migrujících odborech neobsazená již před vznikem DIA. Zároveň bude zásadní, aby nově vládou jmenovaný ředitel DIA, Ing. Martin Mesršmíd[60], a jeho zástupce Ing. Petr Kuchař, ředitel Odboru Hlavního architekta eGovernmentu, efektivním způsobem prosazovaly pro úspěšnou digitalizaci nutné digitalizační projekty.[61] Pokud půjde

[58] Tyto nikoliv interní zdroje jsou známy autorovy práce především díky jeho práce v Odboru kabinetu místopředsedy vlády pro digitalizaci na Úřadu vlády.
[59] Zákon č. 471/2022 Sb., kterým se mění zákon č. 12.2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Důvodová zpráva k tomuto zákona.
[60] Usnesení vlády ze dne 18. ledna 2023 č. 48.
[61] Vize ředitele DIA. In lupa.cz [online]. [cit. 2023-02-26]. Dostupné z: https://www.lupa.cz/clanky/martin-mesrsmid-dia-chci-zaridit-abychom-nemuseli-s-urady-komunikovat-papirove/

vše hladce a bez závažných pochybení, může být účinný nástroj pro efektivní digitalizaci státu již v létě tohoto roku akceschopný.

Digitální a informační agentura bude významně přispívat díky koordinaci digitálních agend k soustavnému zvyšování kybernetické bezpečnosti jako celku, minimálně bude zvyšovat povědomí o kybernetických hrozbách.

DIA však nebude přebírat žádnou ze současných agend NÚKIB. Česká republika tak nebude mít plně jednotnou státní instituci koncentrující všechny digitalizační agendy státu na jedné straně a zabezpečující zároveň i kybernetickou bezpečnosti na straně druhé, jak to má provedené například Estonský úřad pro informační systémy (estonsky *Riigi Infosüsteemide Amet*, oficiální zkratka RIA).[62]

Estonsko slouží pro značnou část států Evropské unie jako určitá inspirace nebo případný vzor pro architekturu eGovernmentu. Je to jeden z mála států, kterému se podařilo za cenu přechodného snížení komfortu a občasných zanedbatelných zásahů do některých práv občanů Estonska, vybudovat plně funkční a centralizovaný úřad koncentrující přehledně všechny digitalizační agendy státu. Estonská RIA je tak vlastně spojený český NÚKIB a česká DIA v jednom. O komparaci těchto zahraničních systémů úřadů zabývající se digitalizací bude autor této práce více pojednávat v kapitolách následujících.

Pro úplnost lze dodat, že dle tohoto změnového zákona[63], organizační struktury Úřadu vlády ČR[64], aktualizovaného nového Statutu Rady pro informační společnost[65] zůstane RVIS a Odbor kabinetu místopředsedy vlády pro digitalizaci, v souladu s touto transformací řízení digitalizace, organizačně na Úřadu vlády. Respektive pro přesnost některé administrativní agendy RVIS se přesouvají z MV na ÚV ČR, a tím RVIS bude organizačně na ÚV ČR nyní již zcela. RVIS a Odboru kabinetu místopředsedy vlády pro digitalizaci budou představovat strategické

[62] Estonský úřad pro informační systémy. In ria.ee [online]. [cit. 2023-01-16]. Dostupné z: https://www.ria.ee/
[63] Zákon č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. §3a.
[64] Organizační schéma Úřadu vlády ČR. In vlada.cz [online]. [cit. 2023-01-16]. Dostupné z: https://www.vlada.cz/cz/urad-vlady/organizacni-struktura/organizacni-schema-uradu-vlady-cr-65949/
[65] Statut Rady vlády pro informační společnost, aktuální znění účinné od 1. 9. 2022. In mvcr.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.mvcr.cz/clanek/rada-vlady-pro-informacni-spolecnost.aspx

řízení a záštitu práce Digitální a informační agentury do doby, než bude DIA schopna sama si strategie a plány a další koncepční záležitosti určovat sama.

Digitální a informační agenturu v této diplomové práci zmiňuji jednak proto, že

- je to vedle Národního úřadu pro kybernetickou a informační bezpečnost jediný odborný ústřední správní úřad, který se v mnohem větší míře bude zabývat digitálním vzděláváním. Zároveň bude prosazovat a nadresortně koordinovat digitalizační agendy a projekty, které v mnoha případech zvyšují nejen UX/UI, ale zprostředkovaně i zvyšují kybernetickou obranyschopnost státu,
- tato práce je možná zcela první závěrečná práce, která o tomto novém ústředním správním úřadu pojednává,
- Digitální a informační agentura bude v mnoha ohledech v úzké součinnosti s NÚKIB a VZ, do struktury DIA se koneckonců inkorporuje celá Správa základních registrů, Odbor eGovernmentu a Odbor Hlavního architekta eGovernmentu, které se podílejí na správě některých kritických informačních systémů veřejné správy.

2.3. Financování

Financování obrany České republiky se navrhuje v době psaní této práce poněkud nelogicky upravit ve dvou zákonech. Ministerstvo obrany ČR na konci roku 2022 navrhlo do právního řádu České republiky přidat samostatný speciální zákon, podle kterého část ustanovení nabude účinností od 1. července 2023 a část od 1. ledna 2024.[66]

V zákoně č. 222/1999 Sb., o zajišťování obrany České republiky, je přitom věnována financování státu celá samostatná část (konkrétně část devátá).[67]

Dle názoru Ministerstva obrany by přijetí nového speciálního zákona s plánovanou účinností od 1. 7. 2023 mělo zjednodušit a zefektivnit systém financování obrany státu.[68] Jako reakci na závazky ČR plynoucí ze Severoatlantické smlouvy a

[66] zatím není známo číslo zákona o financování obrany ČR.
[67] zákon č. 222/1999 Sb., o financování obrany ČR, část devátá.
[68] Nový návrh systemizace financování obrany ČR. In army.cz [online]. [cit. 2022-12-25]. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/ministerstvo-obrany-predstavilo-navrh-noveho-systemu-financovani-strategickych-projektu-239124/

aktuální bezpečnostní situace, nový zákon by měl stanovit minimální objem výdajů na obranu ve výši 2 % HDP, měl by stanovit způsob financování armádních strategických projektů a měl by definovat obranné výdaje, za jejichž řízení bude odpovědné Ministerstvo obrany.

Tato iniciativa plyne z potřeby zajistit dlouhodobé armádní projekty, které mají zásadní dopad na obranyschopnost státu a počítají s rozpočtem nad 300 milionů korun. Strategické projekty by podle navrhované legislativy měla schvalovat vláda, což přinese její intenzivnější zapojení do zajišťování obrany za současného dodržení transparentnosti, nevyužité prostředky bude moci resort obrany převést do dalších let a použít je znovu, až bude určitý projekt připraven.[69]

Vzhledem k současným událostem na východ od České republiky chápe autor této práce tuto potřebu, dovolí si však nesouhlasit s legislativně technickým řešením vytvářet pro tento účel nový samostatný zákon, když se mohl novelizovat přehledně stávající zákon č. 222/1999 Sb., o financování obrany státu, konkrétně jeho část devátá.

2.4. Lidské zdroje

Kvalifikované lidské zdroje, odborníci na IT a kybernetickou bezpečnost jsou z hlediska zajišťování obrany státu v kybernetickém prostoru naprosto klíčovým zdrojem. Bez lidských zdrojů může mít stát dostatek finančních, technických, koncepčních i jiných prostředků, ale bude mu to k ničemu, pokud zde nebudou k dispozici kvalifikovaní specialisté v tomto oboru.

Dle nezávislých statistik je nedostatek kvalifikovaných lidských zdrojů ve státní správě, ale i v soukromém sektoru, stále značně aktuální záležitostí, a to na mnoha úrovních. Poptávka po IT specialistech v posledním roce dokonce ještě stoupla, a to už před rokem 2021 byla značná.[70]

[69] Návrh nového systému financování strategických projektů. In army.cz [online]. [cit. 2023-01-07]. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/ministerstvo-obrany-predstavilo-navrh-noveho-systemu-financovani-strategickych-projektu-239124/

[70] Poptávka po IT odbornících. In novinky.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-v-cesku-chybi-okolo-20-000-it-specialistu-o-40-procent-vic-nez-loni-40407364

Technologie zvyšují nejen bezpečnost, kvalitu života, uživatelskou přívětivost, ale také komfort a konkurenceschopnost státu i firem. Všechny však potřebují zkušené programátory a IT odborníky, které značné množství technologií mají ve svých schopnostech nejen vyrobit, ale i obsluhovat, opravovat nebo udržovat v chodu.

Na tyto důvody a fakt, že poptávka po těchto "ajťácích" značně převyšuje nabídku, již zareagoval soukromý sektor nejen v České republice tím, že zvýšil mzdy těchto IT specialistů. Dle aktuálních statistik je mzda průměrného ajťáka v soukromém sektoru vysoko nad průměrem všech ostatních oborů, a to i nad právníky, bankéři nebo lékaři. Aktuálně se pohybuje kolem 67 tisíc CZK hrubého.[71]

Veřejná správa naproti soukromému sektoru, kde jsou striktnější a rigidnější, tabulková pravidla, na výše uvedené důvody zatím nicméně nezareagovala. Na internetu je poměrně značné množství nabídek práce, kde státní instituce hledají IT specialistu, který by měl mít na nabízenou pozici kromě vysoké školy i znalost cizího jazyka, Microsoft Active Directory, znalost programování atp., s tím, že nabízená odměna bývá na takovou pozici kolem 22 až 35 tisíc CZK hrubého, s nejistým osobním ohodnocením a odměnami.[72]

Místopředseda vlády pro digitalizaci, Ivan Bartoš, sdělil během svého úřadování v roce 2022 v rozhovoru, že *"znalosti, které jsou k digitalizaci potřeba, něco stojí. Je třeba nabízet platy ke sto tisícům korun. Dobrý odborník Vám ušetří miliardu na systému, který by jinak byl navržený špatně"*.[73]Politická vize by v tuto chvíli dle jeho názoru existovala: *"Ve služebním zákoně je třeba změnit platové hladiny pro IT a další vysoce odborné pozice, aby bylo možné do servisní organizace českého eGovernmentu dostat dobře placené odborníky. Kvůli nevůli sáhnout do tabulkových platů ve služebním zákoně se situace ve státním IT řeší*

[71] Plat IT odborníka. In platy.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.platy.cz/platy/informacni-technologie
[72] Odměňování IT specialistů. In diit.cz [online]. [cit. 2023-02-11]. Dostupné z: https://diit.cz/clanek/jaky-je-prumerny-plat-v-it-staci-na-zivot-v-luxusu
[73] IT něco stojí. In lupa.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.lupa.cz/clanky/ivan-bartos-statnim-ajtakum-musime-zvysit-platy-na-sto-tisic-znalosti-neco-stoji/?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu

outsourcováním do podobného typu subjektů, jako jsou IT podniky NAKIT a SPCSS."

Jako další důvod nedostatečného pokrytí lidských zdrojů při snaze o zvyšování kybernetické bezpečnosti České republiky je malý zájem o IT u žen. Dle statistik je mezi "ajťáky" jen 7 % žen, a to i v soukromém sektoru pracuje v IT v ČR ve srovnání s jinými státy EU nejméně žen ze všech států Evropské unie.[74]

[74] Nejméně žen pracuje v českých firmách z celé EU. In mesec.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.mesec.cz/clanky/v-ceskych-firmach-pracuje-nejmene-zen-v-it-v-evrope-horsi-je-jen-madarsko/

3. Vojenské zpravodajství

Faktická odpovědnost zajišťovat obranu a bezpečnost státu, a to i v kybernetickém prostoru, spadá na vládu, která je vrcholným orgánem výkonné moci[75], nikoliv na prezidenta, které je ze své funkce neodpovědný, nikoliv na Poslaneckou sněmovnu Parlamentu České republiky. Vláda je v tomto ohledu odpovědná za své úkoly Poslanecké sněmovně Parlamentu České republiky.[76] Vláda však využívá mnoho ze svých nástrojů, aby své úkoly byla schopna plnit. Kromě Bezpečnostní rady státu a Ústředního krizového štábu využívá jako vrcholný orgán výkonné moci i ozbrojené síly a bezpečnostní sbory a jiné prvky bezpečnostního systému České republiky.

O nejdůležitějších záležitostech týkající se vyhlášení válečného stavu a obrany státu pak rozhoduje Parlament České republiky. Nutný je zde souhlas PSP ČR i Senátu a rozhoduje v tomto ohledu nadpoloviční většina všech poslanců a všech senátorů.[77]

Pro úplnost lze pak zmínit, že na zajišťování bezpečnosti ČR v kyberprostoru se podílí kromě již zmíněných subjektů kromě Ministerstva obrany také Ministerstvo zahraničních věcí, které je odpovědné za znění Bezpečnostní strategie České republiky, a Ministerstvo vnitra, které má ve své struktuře ÚZSI a Policii České republiky (včetně NCOZ SKPV).

O jiných institucionálních nástrojích, které má vláda k dispozici k zajišťování obrany státu v kybernetickém prostoru autor práce pojednal již v kapitole druhé.

Níže si dovolí autor práce pojednat o jedné z nejdůležitějších organizací v oblasti zajišťování České republiky v kyberprostoru.

3.1. Vojenské zpravodajství jako česká státní organizace

Vojenské zpravodajské služby se liší od těch civilních zejména charakterem činnosti a zaměřením na obranu státních celků. Všechny vyspělé demokratické právní státy, které mají alespoň 10 milionů obyvatel (nelze počítat státy jako Island, Vatikán, San Marino atp.) disponují alespoň jednou zpravodajskou

[75] Ústavní zákon č. 1/1993 Sb., Ústava České republiky. Čl. 67. odst. 1.
[76] Ústavní zákon č. 1/1993 Sb., Ústava České republiky. Čl. 68 odst. 1.
[77] Ústavní zákon č. 1/1993 Sb., Ústava České republiky. Čl. 43 ve spojení s Čl. 39 odst. 3.

službou, která se věnuje výhradně obraně státu. Aktivity vojenských ZS hrají zásadní a nenahraditelnou roli při zajišťování informovanosti oprávněných adresátů v případě hrozícího či nastalého bezprostředního vojenského konfliktu.

Autor této práce v následujících podkapitolách rozvede téma české vojenské zpravodajské služby, která je z hlediska zajišťování obrany státu v kybernetickém prostoru nezastupitelná.

Vojenské zpravodajství ČR je jediná česká vojenská zpravodajská služba[78], která ve vojenské působnosti koncentruje rozvědnou i kontrarozvědnou činnost. Vznikla sloučením dvou dnes již neexistujících vojenských zpravodajských služeb, Vojenského obranného zpravodajství, což byla vojenská rozvědka, a Vojenské kontrarozvědky. Tyto dvě ZS existovaly i před sametovou revolucí a v nové uspořádáním společnosti po roce 1989 si ponechaly svoje původní názvy. Proces slučování dvou předchozích vojenských ZS byl formálně dokončen v roce 2005 přijetím zákona č. 289/2005 Sb., o Vojenském zpravodajství.

Vojenské zpravodajství neřadí žádný právní předpis ČR mezi bezpečnostní sbory. Příslušníci VZ, které je dle zákona o ZS součást Ministerstva obrany[79], jsou vojáci z povolání, vojáci v záloze povoláni k výkonu vojenské činné služby k VZ nebo zaměstnanci zařazení ve Vojenském zpravodajství. Služební poměr příslušníků VZ se na rozdíl od služebního poměru příslušníků BIS a ÚZSI řídí zákonem č. 221/1999 Sb., o vojácích z povolání. Vojenské zpravodajství tak je spíše řazeno mezi složky ozbrojených sil ČR.

Vzhledem k povaze neohraničeného kybernetického prostoru často v době útoku nelze odlišit původ útoku, a zda se jedná o vnější či vnitřní napadení. Stejně tak není možné zcela jasně vyhodnotit, zda již jde o útok zakládající právo na sebeobranu ve smyslu zákona o VZ[80] či případně dle Washingtonské smlouvy[81] nebo zda se jedná o čin charakteru teroristického, kriminálního nebo např.

[78] Zákon č. 289/2005 Sb., o Vojenském zpravodajství. § 2.
[79] Zákon č.153/1994 Sb., o zpravodajských službách ČR. § 3 písm. c).
[80] Zákon č. 289/2005 Sb., o Vojenském zpravodajství. především § 16f a 16g.
[81] Washingtonská smlouva z 4. dubna 1949. čl. 5.

špionážního.[82] Nejvhodnější a nejlogičtější je proto svěřit úkol zajišťovat obranu v kyberprostoru zpravodajským službám. Ty se totiž podílí na zajišťování bezpečnostních zájmů národního státu v celém bezpečnostním spektru.

Právě Vojenskému zpravodajství České republiky byl dle posledních novel jeho zřizovacího zákona svěřen díky nově získaným kompetencím úkol zajišťovat obranu České republiky v kyberprostoru. Proto autor práce rozvede tuto zpravodajskou službu v širším rozsahu než zbylé dvě ZS ČR zmíněné v kapitole 2.2. o institucionálních nástrojích České republiky. Úkolem VZ ČR je sběr, analýza a šíření informací týkajících se kybernetické bezpečnosti a obrany ČR v kybernetickém prostoru, a to jak v rámci České republiky, tak i v zahraničí.

Rozhodnutí udělit úkol zajišťovat obranu státu v kyberprostoru, pro něhož jsou státní hranice defakto irelevantní, ze všech ZS ČR právě VZ je logické minimálně ze dvou dalších důvodů. Za prvé jelikož tato česká ZS narozdíl od BIS a ÚZSI působí jak v tuzemsku, tak v zahraničí. Za druhé VZ ČR je součástí Ministerstva obrany a má tak úzké vazby na všechny složky ozbrojených sil České republiky, kteréžto složky se mohou díky činnosti VZ navzájem podporovat.

Zákon o VZ byl k datu 27. 2. 2023 novelizován celkem devětkrát. Z hlediska tématu této diplomové práce je zásadní poslední novela, zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony, s nabytím účinnost k 1. 7. 2021.

Zákon č. 150/2021 Sb. zákon o VZ významně doplnil o kapitolu čtvrtou, která nese název *“Činnosti vojenského zpravodajství při zajišťování obrany České republiky”*. Ačkoliv to nemá tato kapitola přímo ve svém názvu zmíněné, zabývá se ve svých 13 paragrafech obranou státu v kybernetickém prostoru.[83]

Změnový zákon, který během svého legislativního procesu prošel řadou výrazných úprav, zejména během meziresortního připomínkového řízení, navazuje na v roce 2016 ve Varšavě schválenou strategii NATO, na Bezpečnostní strategii ČR z roku 2015 a na Národní strategii kybernetické bezpečnosti ČR

[82] Proč právě Vojenské zpravodajství? In vzcr.cz [online]. [cit. 2023-03-04]. Dostupné z:https://vzcr.cz/kyberneticka-obrana-46
[83] Zákon č. 289/2005 Sb., o Vojenském zpravodajství. § 16a a dále.

vypracovaná NÚKIB a schválena vládou. Účinné znění má ambici významně posílit a doplnit akceschopnou obranu státu vůči nejzávažnějším kybernetickým útokům.

3.2. Činnost Vojenského zpravodajství

Jednou z hlavních činností Vojenského zpravodajství v oblasti kybernetické bezpečnosti je sledování kybernetických hrozeb a rizik. VZ monitoruje různé typy kybernetických útoků, jako jsou například phishingové útoky, útoky pomocí škodlivého softwaru a útoky na kritickou infrastrukturu. Dále se zabývá analýzou těchto útoků a vytvářením strategií na jejich zajištění a prevenci.

Vojenské zpravodajství se také věnuje sběru informací o kybernetických aktivitách cizích států (zejména vně NATO) a teroristických organizací. Informace o aktivitách relevantních států jsou velmi cenné, jelikož mohou posloužit jako významný zdroj inspirace, prevence a efektivnější připravenosti na všechny možné typy útoků.

Další důležitou činností Vojenského zpravodajství v oblasti kybernetické bezpečnosti je spolupráce s dalšími tuzemskými orgány státní správy v oblasti kybernetické obrany.[84] Asi nejdůležitější je spolupráce s NÚKIB, ostatními ZS, NBÚ a dalšími bezpečnostními prvky bezpečnostního systému ČR. Vojenské zpravodajství ale spolupracuje také s dalšími zpravodajskými službami a složkami ozbrojených sil České republiky i spojeneckými ozbrojenými silami členských států NATO.

V organizační struktuře armády České republiky se totiž významně podílí na kybernetické obraně i Velitelství kybernetických sil a informačních operací (zkratkou VeKySIO), které působí nezávisle, společně nebo v součinnosti s pozemními, vzdušnými či speciálními složkami ozbrojených sil České republiky. Činnosti VeKySIO a VZ se doplňují a vzhledem ke společné struktuře pod Ministerstvem obrany ČR mohou své aktivity efektivně koordinovat.

Z těchto výše zmíněných subjektů však VZ nejvíce koordinuje aktivity zaměřené na zajištění kybernetické bezpečnostních zájmů České republiky se všeobecně

[84] Obranná strategie České republiky z roku 2017. Pilíř 2, bod 28.

známým a již organizačně připraveným NÚKIB, aby mohlo být co nejúčinněji řešeno riziko kybernetických útoků a zajištěna maximální ochrana, předávání a případného zužitkování utajovaných informací. Příkladem může být společné vydání doporučení pro cestující české sportovce a veřejnost.[85]

Kromě toho se VZ aktivně účastní ve spolupráci s výše jmenovanými subjekty výzkumných projektů zaměřených na oblast zajišťování kybernetické obrany státu. V neposlední řadě VZ vyvíjí a implementuje nejmodernější technologie na zajištění kybernetické bezpečnosti a kybernetické obrany, a to jak pro potřeby ozbrojených sil ČR, tak i pro další složky státní správy.

Aby si VZ ČR udržela místo v poměrně silné konkurenci zahraničních ZS ČR musí v rámci své práce používat nejúčinnější nástroje pro efektivní sběr, analýzu a vyhodnocování informací. To může pochopitelně narážet na určité lidskoprávní limity, které jsou garantovány všem občanům demokratických právních států.

Vojenské zpravodajství České republiky tak hraje klíčovou roli v zajištění bezpečnosti a obrany České republiky v kybernetickém prostoru a jeho činnost je nezbytná pro ochranu kritické infrastruktury, ochranu utajovaných informací a ochranu utajovaných informací. Jeho práce je nezbytná pro ochranu kritické infrastruktury, utajovaných informací, a významně přispívá ke zdraví a spolehlivosti celkového bezpečnostního systému státu.

Jelikož Vojenské zpravodajství koncentruje rozvědnou i kontrarozvědnou vojenskou činnost, patří mezi jeho úkoly i zajišťovat zpravodajské informace o ozbrojených silách a jiných bezpečnostních prvků cizích států. Zajišťuje získávání zpravodajských informací také ohledně koncepčních, komunikačních a finančních nástrojích cizích mocností.

V dnešní době propracovaného systému auditu, rozpoznávání obličejů a identity všech občanů vyspělých států je třeba uvést, že dříve preferovaná a možná hojně používaná metoda získávání zpravodajských informací pomocí infiltrace by dnes již mohla být neefektivní, teoreticky riskantnější a obtížně proveditelná. Z tohoto

[85] Doporučení pro české olympioniky i veřejnost. In nukib.cz [online]. [cit. 2023-02-27]. Dostupné z:https://www.nukib.cz/cs/infoservis/doporuceni/1792-nukib-vydal-spolu-s-vojenskym-zpravodajstvim-doporuceni-pro-ceske-olympioniky-i-verejnost/

důvodu by dle názoru autora práce mělo VZ směřovat ofenzivní část své činnosti výhradně do kybernetického prostoru, jelikož odhalená operace infiltrace určitého zpravodajského důstojníka v cizí zemí by mohla přinést České republice mnohem více škody než užitku. Stát, který by agenta odhalil, by ho mohl nejen využívat k těžení informací prostřednictvím podrobných výslechů, ale také by ho mohl použít jako nástroj propagandy a důkazu, že proti České republice jsou díky tomuto selhání příslušníka VZ oprávněni přikročit k patřičným reakcím.

Taková nadbytečná provokace by mohla být navíc posuzována jako útok na určité bezpečnostní zájmy daného státu a nejenže by mohl stát následně přerušit diplomatické styky s ČR, ale zároveň by díky případně eskalaci mohla být ohrožena sama ČR, pokud by poškozený stát byl mnohem mocnější. Lze také uvést, že by touto operací mohl být ohrožen život nebo psychické či fyzické zdraví cizím státem odhaleného zpravodajského důstojníka.

Pokud by se nicméně skutečně přihodilo, že určitý příslušník VZ zůstane neodhalen v cizím státě, mohly by být umístění a činnost takové osoby díky případně získaným cenným zpravodajským informacím značně výhodné pro všechny státy Severoatlantické aliance.

Kromě obranných a útočných činností lze činnost VZ dělit i na:

- koncepční,
- strategickou,
- taktickou a
- operativní.

3.3. Možnosti obrany při kybernetických útocích na Českou republiku

Zmiňovaná novela zákona o VZ v předchozí podkapitole přiznává VZ v kybernetickém prostoru výsadní postavení mezi českými ZS. VZ totiž nyní může zejména:

A. získávat poznatky o kybernetických útocích a hrozbách,

B. cíleně detekovat kybernetické útoky a

C. v neodkladných případech na ně adekvátně reagovat.

Tato novelizace vychází z požadavků strategie vytvořené NÚKIB a schválené vládou ČR, zároveň také z požadavků vyplývající z Bezpečnostní strategie z roku 2015 a vyplývající také z Národní strategie kybernetické bezpečnosti České republiky.[86] NATO mimo jiné rovněž uznala ve svých koncepčních dokumentech kromě vesmíru i kybernetický prostor za vysoce aktuální operační doménu zpravodajských služeb. V případě kybernetického prostoru se tak stalo již v roce 2016 na summitu ve Varšavě.[87] Požadavek na posílení kybernetické bezpečnosti státu je předmětný také kvůli aktuálnímu úsilí digitalizace státní správy ČR a vzniku Digitální a informační agentury jako nového ústředního správního úřadu.[88]

V rámci zajišťování kybernetické obrany státu má od novelizace zákona o VZ nyní možnost požadovat od poskytovatelů připojení či provozovatelů online služeb metadata o provozu. Těmito metadaty jsou myšleny např. porty, IP adresy, tedy jedničné identifikace počítačů v internetové síti, velikost maximálně přenášených dat atp. V ideálním případě by si relevantní soukromoprávní právnické osoby mohly s VZ předávat tyto metadata.

V rámci monitoringu síti má VZ také možnost do těchto sítí spravovaných nebo provozovaných soukromou organizací umisťovat nástroje detekce, tedy sondy.

Zákon o VZ v účinném znění nicméně zakazuje sledovat online komunikaci. To by již představovalo příliš velký zásah do základních práv a lidských svobod zmíněných v Listině základních práv a svobod.[89]

3.4. Národní centrum kybernetických operací

Vojenské zpravodajství od roku 2016 ve své struktuře rozvíjí tzv. Národní centrum kybernetických operacích (zkratkou NCKO). NCKO bude vhodným nástrojem pro efektivnější pro zabezpečení a exekuci všech v předchozích podkapitolách zmíněných pravomocích VZ. Zákon s tímto organizačním útvarem explicitně

[86] Národní strategie kybernetické bezpečnosti.
[87] Summit NATO ve Varšavě. In natoaktual.cz [online]. [cit. 2023-03-04]. Dostupné z: https://www.natoaktual.cz/projekty/special-summit-nato-ve-varsave-2016.A160405_144542_na_zpravy_m02
[88] Zákon č. 2/1969 Sb., kompetenční zákon. § 2, bod 19.
[89] Listina základních práv a svobod České republiky, zejména čl. 7, 8 a 10 ve spojení s čl. 3 odst. 3 a s čl. 4 odst. 2, 3 a 4.

nepočítá, nicméně z ustanovení je patrné, že bude muset VZ přijmout určitá opatření, aby mohlo efektivně naplnit záměr zákonodárce.

Národní centrum kybernetických operací již sice zaregistrovalo novou doménu ncko.cz, nicméně vlastní webové stránky zatím funkční nemá a ncko.cz nyní stále přesměrovává na hlavní web VZ vzcr.cz.[90] Jako součást Ministerstva obrany bude muset stejně migrovat na jednotnou doménu *.gov.cz, tudíž bude muset být doména ještě aktualizována. O záměru migrace na jednotnou státní doménu *.gov.cz bude autor práce pojednávat v kapitole páté a v závěru.

Informace o reálném plnění svěřených úkolu této zpravodajské služby nejsou (a neměly by být) z povahy věci veřejnosti přístupné.

Svěřené pravomoci VZ, s kterými se pojí i velká odpovědnost, v této oblasti podléhají kontrole ze strany k tomu zřízenému novému institutu. Tímto kontrolním orgánem je inspektor pro kybernetickou obranu.

3.5. Kontrola Vojenského zpravodajství

Vzhledem k nově přiznaným pravomocem VZ po detekci bezprostředního nebezpečí kybernetického útoku zasáhnout v neodkladných případech a teoreticky tak v obranné reakci zasáhnout do základních lidských práv a svobod občanů je potřeba tyto činnosti kontrolovat.

O kontrole činnosti zpravodajských služeb, včetně kontroly činnosti Vojenského zpravodajství autor této práce pojednal již ve své předchozí diplomové práce, která přímo nesla název *“Zpravodajské služby a kontrola jejich činnosti se zaměřením na Českou republiku”*.

Nepočítaje vnitřní kontrolní mechanismy, lze v širším pojetí uvažovat hned o několika úrovních vnějších kontroly.

Zpravodajské služby ČR kontrolují nebo by měli kontrolovat mimo jejich vlastní kontrolní mechanismy tyto subjekty:

- Vláda ČR,

[90] Národní centrum kybernetických operacích. In ncko.cz [online]. [cit. 2023-03-04]. Dostupné z: https://www.ncko.cz/

- Poslanecká sněmovna Parlamentu ČR,
- Orgán nezávislé kontroly,
- Prezident ČR a
- Soudy, zejména vrchní soudy.

O kontrolách ze strany těchto subjektů autor této práce podrobně pojednal ve své předchozí diplomové práci psanou na Právnické fakultě Univerzity Karlovy, tudíž jejich kontrolní činnost zde nebude podrobněji rozepisovat.

Je ale na místě uvést, že např. Orgán nezávislé kontroly od doby, kdy byla autorova minulá diplomová práce na PrF UK dopsána, zůstává stále neobsazen, tudíž zde žádná kontrola ze strany tohoto orgánu ani nemůže probíhat. Vzhledem k tomu, že současná vláda nijak neaktualizovala zákon č. 90/1995 Sb., jednací řád Poslanecké sněmovny, lze se domnívat, že díky aktuálnímu politickému dění[91] a rychlosti přijímání legislativy a rozhodnutí Poslanecké sněmovny Parlamentu ČR, se ještě Orgán nezávislé kontroly zřejmě dlouho neobsadí. Např. schválení programu schůze trvalo v některých případech přes 30 hodin.[92]

Co se týká kontrolní činnosti jiných výše jmenovaných orgánů, je situace rovněž nezměněná. A dle názoru autora práce rovněž nevyhovující, zejména co se parlamentní kontroly činnosti ZS prostřednictvím komisí složených z poslanců týče.

Je tedy více než žádoucí, aby nad rámec stávající úpravy a obecných kontrolních mechanismů tu existovala kontrola speciálním orgánem pouze pro oblast kyberprostoru. Na tuto potřebu se během novelizování zákona o VZ myslelo a zřídil se tak nový monokratický orgán inspektora pro kybernetickou obranu, kterého odvolává a jmenuje vláda ČR na návrh ministra obrany.

Jako první v této funkci stanul Mgr. Jan Vacek, uznávaný odborník v oblasti legislativy, informačních technologií a kybernetické bezpečnosti, kterého po

[91] Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny. § 50 a násl., kapitola o schůzích a jednáních PSP ČR.
[92] Schválení programu schůze za 30 hodin. In iprima.cz [online]. [cit. 2023-03-04]. Dostupné z: https://cnn.iprima.cz/snemovna-po-30-hodinach-schvalila-program-schuze-k-nizsimu-rustu-penzi-201789

návrhu ministryně obrany, Černochové, vláda jmenovala svým usnesením[93] ze dne 6. 4. 2022.

Inspektor je formálně příslušníkem Vojenského zpravodajství a bude podřízen přímo ministryni obrany.

Hlavní úkoly inspektora pro kybernetickou obranu dle zákona o VZ jsou tyto:

a) *prověřuje správnost postupů Vojenského zpravodajství při činnostech, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, pokud se týkají zabezpečení ochrany dat a informací,*

b) *ověřuje účinnost opatření přijatých Vojenským zpravodajstvím za účelem zajišťování ochrany dat a informací zpracovávaných při činnostech, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, podílí se na jejich zavádění do činnosti Vojenského zpravodajství a navrhuje jejich případnou aktualizaci,*

c) *při činnostech Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, poskytuje na vyžádání poradenskou podporu příslušníkům Vojenského zpravodajství v oblasti ochrany dat a informací,*

d) *za účelem zajištění účinnosti opatření přijímaných k ochraně práv spolupracuje se subjekty, u nichž byly umístěny nástroje detekce podle."*[94]

Inspektor pro kybernetickou obranu je jmenován na dobu pěti let. Dle zákona[95] je vázán pouze zákonem a je povinen tuto kontrolní činnost vykonávat nezávisle. Jak již však bylo výše uvedeno, je přímo podřízen ministryni obrany a je defakto příslušníkem VZ. Tato nezávislost díky tomu je poněkud omezená, a spíš než o vnější kontrolu této ZS se jedná dle autora práce spíše o vnitřní kontrolu organizace, která je svým uspořádáním skrytá občanům a vnějším pozorovatelům. Toto řešení tedy může dle názoru autora práce explicitně řečeno vypadat poněkud netransparentně.

[93] Usnesení vlády ze dne 6. dubna 2022 č. 274.
[94] Zákon č. 289/2005 Sb., o Vojenském zpravodajství. § 16l odst. 1.
[95] Zákon č. 289/2005 Sb., o Vojenském zpravodajství. § 16k odst. 5.

Ministryni obrany je povinen předávat minimálně 1x za pololetí zprávu o všech zjištěných nedostatcích VZ při zajišťování obrany České republiky v kybernetickém prostoru.

4. NATO a komparace obranyschopnosti v kyberprostoru

Tehdejší prezident ČR, Václav Havel, podepsal 26. února 1999 listiny o přistoupení ČR k Severoatlantické smlouvě. Tímto aktem se Česká republika stala plnohodnotným členským státem NATO a vzala tak na sebe nejen výhodu strategické obrany ale i povinnosti z této skutečnosti vyplývající.

Česká republika se tak navrátila mezi společenství demokratických právních států, mezi které patřila i v období První republiky. Stalo se tak navzdory neformálnímu slibu uzavřenému mezi vítězi druhé světové války, že se NATO nebude dál rozšiřovat na východ.

Se sjednocením Německa vyjádřili souhlas podpisem smlouvy o státní suverenitě sjednoceného Německa spojenci ve druhé světové válce, tedy SSSR, USA, Velká Británie a Francie na konferenci 12. září 1990 v Moskvě nesoucí název *formát 2+4* neboli *konference dva plus čtyři*.[96] Tato mezinárodní smlouva v zahraničí bývá nazývána také tzv. *Treaty on the Final Settlement with Respect to Germany* nebo *Two Plus Four Agreement*. Čtyřmi jsou míněni 4 stěžejní vítězné velmoci a dvěma jsou míněny vlády Spolkové republiky Německo a vlády Německé demokratické republiky. Během této dohody bylo slíbeno, že při stažení tehdejších sovětských vojsk nebude NATO rozšiřováno dále na východ, tzv. *"not one inch eastward" promise* (přeloženo *"ani jeden palec východně" slib*).[97]

Na nedodržení tohoto slibu a dohody se často odkazuje současná vláda Ruské federace jako hlavního nástupnického státu SSSR. Ruská federace v době psaní této diplomové práce představuje díky událostem na Ukrajině a faktické okupování velkého části jejího území Ruskou federací současnou nejvýznamnější bezpečnostní kybernetickou hrozbu pro státy Severoatlantické aliance. Ruská federace je společně s Íránem a Čínskou lidovou republikou vojenskou velmocí disponující kromě rozvinuté sítě kybernetických specialistů jadernými zbraněmi,

[96] Two plus four agreement. In treaties.un.org [online]. [cit. 2023-02-18]. Dostupné z: https://treaties.un.org/doc/Publication/UNTS/Volume%201696/volume-1696-I-29226-English.pdf
Srov. Dohoda 2+4. ct24.ceskatelevize.cz [online]. [cit. 2023-02-18]. Dostupné z: https://ct24.ceskatelevize.cz/archiv/1443337-znovusjednoceni-nemecka-historicky-podpis-smlouvy-2-4

[97] Promise to Gorbachev. nsarchive.gwu.edu [online]. [cit. 2023-02-18]. Dostupné z: https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early

které by mohly být pro státy NATO v budoucnu výzvou. Ruská federace na rozdíl od Íránu a Čínské lidové republiky v době psaní této diplomové práce okupuje stát sousedící s východním křídlem NATO a EU a je ze všech vojenských velmocí k České republice geograficky nejblíže.

Politická reprezentace Ruské federace je také jedinou politickou reprezentací určité vojenské velmoci, která se opakovaně vyjadřovala nikoliv přátelsky k České republice. Stěžejním příkladem budiž zařazení (jako vůbec první země) České republiky po bok USA do seznamu zemí Ruské federaci nikoliv přátelských v květnu roku 2021.[98] Po uvalení sankcí na Ruskou federaci byl tento seznam rozšířen o dalších 46 zemí. Momentálně jsou na seznamu všechny státy Evropské unie, a pro zajímavost i všechny státy G7.[99] RF a některé vlastenecké organizace RF, ke kterém čelní představitelé RF nebo jejich zástupci vyjadřovali v minulosti opakovaně podporu, byly také orgány ČR opakovaně obviněné z podezření kybernetických útoků na státní instituce České republiky.[100]

Kvůli výše uvedeným důvodům bude během komparace obrany v kybernetickém prostoru států NATO zmiňovány i jiné velmoci v oblasti kyberprostoru a možnosti dialogu s nimi.

4.1. NATO Cooperative Cyber Defense Center of Excellence

NATO se v závislosti na rapidním vývoji informačních technologií v posledních letech zaměřuje stále více na kybernetickou bezpečnost, což zahrnuje ochranu svých sítí, systémů a dat před kybernetickými hrozbami nejrůznějšího charakteru. NATO má pro tento účel vytvořený orgán, kterým je tzv. *NATO Centrum pro kybernetickou obranu*, kterým je jedním z tzv. *Center excelence* (zkratkou NATO CCDCOE).[101]

---

[98] Rusko rozšířilo seznam nikoliv přátelských zemí. In forbes.cz [online]. [cit. 2023-02-18]. Dostupné z: https://forbes.cz/rusko-rozsirilo-seznam-nikoliv-pratelskych-zemi-sve-financni-zavazky-jim-bude-splacet-jen-v-rublech/

[99] Aktuální seznam nikoliv přátelských zemí dle ruských zdrojů. In ria.ru [online]. [cit. 2023-02-18]. Dostupné z: https://ria.ru/20220722/nedruzhestvennye_strany-1804332755.html?in=t

[100] Russia behind cyber attacks on websites. In english.nv.ua [online]. [cit. 2023-03-11]. Dostupné z: https://english.nv.ua/nation/russia-behind-cyber-attack-on-candidates-websites-during-presidential-elections-in-czech-republic-50297339.html

[101] NATO Centrum pro kybernetickou obranu. In ccdcoe.ru [online]. [cit. 2023-03-04]. Dostupné z: https://ccdcoe.org/

NATO CCDCOE bylo založeno v roce 2008 s hlavním úkolem poskytovat poradenství, školení IT odborníků a výzkum v oblasti kybernetické bezpečnosti pro členské státy NATO. NATO CCDCOE spolupracuje s vojenskými a civilními expertními týmy ze všech členských států NATO a jiných zemí, a to včetně civilních sektorů, akademických institucí a průmyslových partnerů.

NATO CCDCOE má několik hlavních kompetencí v oblasti kybernetické obrany:

A. provádí výzkum a vývoj v oblasti kybernetické obrany a poskytuje expertní znalosti pro vývoj politik a strategií NATO v této oblasti.

B. poskytuje školení a cvičení pro vojáky a civilní pracovníky z členských států NATO, aby se mohli efektivněji bránit kybernetickým hrozbám.

C. poskytuje poradenství a konzultace pro členské státy NATO v oblasti kybernetické bezpečnosti, včetně analýzy rizik a posouzení bezpečnostních opatření.

D. podílí se na vytváření standardů a certifikací v oblasti kybernetické bezpečnosti, aby se zajistilo, že vojenské i civilní organizace NATO dodržují nejvyšší bezpečnostní standardy.

Celkově lze říci, že NATO CCDCOE je klíčovým orgánem pro koordinaci a poskytování expertních znalostí v oblasti kybernetické bezpečnosti pro členské státy NATO. Centrum hraje důležitou roli při zajišťování ochrany kybernetického prostoru a zvyšování úrovně kybernetické bezpečnosti v rámci NATO i mimo něj.

4.2. Evropská unie

Podobně jako NATO i Evropská unie má ve své struktuře orgány zabývající se kybernetickou bezpečností. Autor práce si v této souvislosti dovolí i srovnat členské státy Evropské unie ve vyspělosti v oblasti kybernetické obranyschopnosti.

4.2.1. ENISA

Jedním z nejdůležitějších organizací v rámci EU pro kybernetickou bezpečnost je bezpochyby *The European Union Agency for Cybersecurity*, česky *Agentura pro kybernetickou bezpečnost Evropské unie* (zkratkou ENISA), který byla založena

již v roce 2004 jako nezávislá agentura EU s cílem poskytovat poradenství a podporu v oblasti kybernetické bezpečnosti pro členské státy EU.

ENISA zejména:

A. poskytuje poradenství a podporu pro členské státy EU v oblasti kybernetické bezpečnosti, včetně analýzy rizik, posouzení bezpečnostních opatření a vytváření strategií,

B. poskytuje školení a cvičení pro odborníky na kybernetickou bezpečnost z členských států EU, aby se zlepšila jejich schopnost reagovat na kybernetické hrozby,

C. shromažďuje a analyzuje informace o kybernetických hrozbách, aby poskytovala předpovědi a doporučení pro členské státy EU a

D. podílí se na vytváření standardů a certifikací v oblasti kybernetické bezpečnosti, aby se zajistilo, že organizace v EU dodržují nejvyšší bezpečnostní standardy.

ENISA mimo jiné spolupracuje s členskými státy EU, dalšími evropskými agenturami a dalšími organizacemi na celém světě. Pro zajišťování bezpečnosti kybernetického prostoru EU hraje ENISA významnou úlohu.[102]

4.2.2. Cyber Coalition

V souvislosti s členskou zemí Evropské unie by autor této práce rád vyzdvihl recentní událost konanou od 28. 11. 2022 do 2. 12. 2022 jednoho z nejvýznamnějších světových cvičení 26 členských států NATO zaměřeného na kybernetickou bezpečnost tentokrát v Tallinnu, hlavního města Estonska, známého jako *Cyber Coalition 2022*, kteréžto cvičení se pořádá již po dvanácté.[103]

Česká republika se v roce 2022 zúčastnila tohoto cvičení již po dvanácté, od svého založení ČR zastupuje Národní úřad pro kybernetickou a informační bezpečnost, který obvykle pomáhá i s přípravou této mezinárodní akce. Cyber Coalition cvičení je založeno na komplexním a realistickém scénáři, kdy se tým A (složený se

[102] ENISA. In enisa.europa.eu [online]. [cit. 2023-03-04]. Dostupné z: https://www.enisa.europa.eu/
[103] Cyber Coalition 2022. In nato.int [online]. [cit. 2023-02-11]. Dostupné z: https://www.act.nato.int/cyber-coalition

zástupců určitých členských států) snaží v simulovaném prostředí aktivně ohrozit misi NATO nebo jiné členské státy prostřednictvím všech dostupných kybernetických prostředků a tým se snaží těmto útokům aktivně zamezit nebo předejít. Obdobně jako v rámci České republiky cvičí aktuálně Národní centrum kybernetických operací, které se vytváří po poslední novele zákona o Vojenském zpravodajství v rámci struktury Vojenského zpravodajství.[104]

Tyto útoky v reálně simulovaném virtuálním prostředí Cyber Range pomáhají ve značné míře všem členským státům si rozšířit povědomí identifikovat případné netušené hrozby či rizika a ve značné míře zvyšují prevenci a připravenost bezpečnostních složek na tyto skutečné kybernetické výzvy, včetně útoků na kritickou infrastrukturu.[105]

V Estonsku je hlavním orgánem pro zajišťování kybernetické obrany státu protějšek českého NÚKIB, estonská RIA, která je ovšem starší, zkušenější a dle mezinárodních srovnání i efektivnější zatím než český NÚKIB. RIA má na starosti současně i digitalizační agendy. O RIA bylo již pojednáno v kapitole 2.2.4. této práce.

Jak již bylo předesláno v kapitole druhé, Estonsko je jeden z lídrů Evropské unie, co se využívání digitálních služeb občany a vysoké úrovně kybernetické bezpečnosti státu týče.

4.2.3. DESI

Dle DESI (anglicky *Digital Economy and Social Index*) se sice Estonsko umisťuje “až” na 9. místě, jelikož průměr tohoto indexu poněkud rapidně snižuje pokrytí pevného a mobilního širokopásmového připojení (4G a 5G síť) po celé zemi.[106] Podle “connectivity” je tak Estonsko až na 26. místě ze zemí Evropské unie, což je předposlední místem, na chvostu je v tomto kritériu překvapivě Belgie (která má ale jiné 3 kritéria nad průměrem EU). Estonsko je však zcela nejlepší v kritériu

[104] Kybernetická obrana České republiky. In vzcr.cz [online]. [cit. 2023-02-12]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46
[105] Cvičení NATO ohledně obranyschopnosti aliance v kybernetickém prostoru. In nukib.cz [online]. [cit. 2023-02-12]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1917-experti-nato-na-kybernetickou-bezpecnost-v-estonsku-pracovali-na-spolupraci/
[106] Estonsko v DESI indexu. In europa.eu [online]. [cit. 2023-02-12]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-estonia

poskytovaných digitálních služeb (e-Government, e-Health, e-Recept, e-Land, e-Ticket atp.).

Nejlepší země dle tohoto poměrně prestižního srovnání států EU, DESI, jsou skandinávské země a nejhorší Bulharsko a Rumunsko.

Co se kybernetické bezpečnosti týče, explicitně s tímto kritériem DESI nepočítá, což je také další důvodem, proč se Estonsko umístilo přes svou pověst digitálního lídra nikoliv na špici.

Česká republika se umisťuje v DESI v té horší polovině srovnatelně s Itálií.

4.3. Celosvětové srovnání zemí z hlediska kybernetické bezpečnosti

Mnohem zajímavějším srovnání je tzv. *Global cybersecurity index*, který srovnává všechny země světa v tématu kybernetické bezpečnosti a který zpracovává Mezinárodní telekomunikační unie.[107] Estonsko je v tomto srovnání zemí 3. nejlepší, za Spojenými státy americkými, Velkou Británií a Saúdskou arábií, kteréžto dva poslední jmenované státy dle indexu obsazují druhé místo.[108] S přihlédnutím k tomu, že Velká Británie již není členským státem Evropské unie je Estonsko oficiálně nejvyspělejším státem Evropské unie, co se kybernetickém bezpečnosti týče.

Podle šetření Global Cybersecurity Index v roce 2020 se Česká republika sice umístila na 34. místě z celkového počtu 194 států, což je relativně dobrý výsledek, nicméně nepočítaje státy jako Vatikán, San Marino, některé balkánské státy nebo např. Monako, což je stát o 2,02 km^2, obsazuje Česká republika dle tohoto indexu v kontrastu s Estonskem ze všech vyspělejších států Evropské unie nejhorší hodnocení, v podstatě chvostu žebříčku.[109] Na toto hodnocení České republiky lze tedy nahlížet z více úhlů pohledu.

Navíc existují i jiné indexy jako např. tzv. National cyber security index (zkratkou NCSI) dle kterého se Česká republika umisťuje zejména díky velmi dobré práci

[107] Mezinárodní telekomunikační unie. In itu.int [online]. [cit. 2023-02-12]. Dostupné z: https://www.itu.int/en/Pages/default.aspx
[108] Estonia 3. world best in cybersec. In e-estonia.com [online]. [cit. 2023-02-12]. Dostupné z: https://e-estonia.com/estonia-outranks-most-of-the-world-in-global-cybersecurity-index/
[109] Global Cybersecurity Index. In itu.int [online]. [cit. 2023-02-12]. Dostupné z: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

zaměstnanců zmiňovaného NÚKIB v posledních letech dokonce na 5. místě ze všech zemí světa. To je vynikající hodnocení, jednu příčku za Estonskem a před skandinávskými státy, před Německem, USA nebo před Velkou Británií.[110]Jako každá země, ČR stále čelí různým výzvám a hrozbám, jako jsou kybernetické útoky, šíření dezinformací a kradení dat. Proto je důležité, aby ČR i nadále investovala do své kybernetické bezpečnosti a spolupracovala s jinými zeměmi na mezinárodní úrovni, zní z doporučení těchto šetření.

4.4. Spojené státy americké

Spojené státy americké jsou jednou z nejvyspělejších zemí v oblasti kybernetické bezpečnosti (dle Global cybersecurity index obsazují první místo) a patří dlouhodobě mezi hlavní cíle teroristických útoků v oblasti kyberprostoru ze strany států, které nejsou členy NATO, i ze strany nezávislých aktérů. V roce 2021 americká vláda oznámila několik iniciativ a strategií zaměřených na zlepšení kybernetické bezpečnosti, včetně strategie pro zajištění kybernetické bezpečnosti národní infrastruktury a nového zákona o kybernetické bezpečnosti.[111]

USA disponují širokou škálou nástrojů a programů zaměřených na boj proti kybernetickým hrozbám, jako například Národním centrem pro kybernetickou bezpečnost (anglicky National Cybersecurity Center), které má dle názoru autora práce zdařilý web,[112] a Národním institutem pro standardy a technologie (National Institute of Standards and Technology)[113], které poskytují směrnice a standardy pro ochranu informačních systémů. Zároveň USA spolupracují s mezinárodními partnery a organizacemi v oblasti kybernetické bezpečnosti, jako například s NATO a Organizací pro hospodářskou spolupráci a rozvoj (OECD).

4.4.1. The National Security Agency

V překladu do češtiny tzv. Agentura národního bezpečnosti nebo také Národní bezpečnostní agentura (dále také “NSA”) je americká federální vládní

[110] Hodnocení všech států světa v kybernetické bezpečnosti. In ncsi.ega.ee [online]. [cit. 2023-03-11]. Dostupné z: https://ncsi.ega.ee/ncsi-index/?order=rank
[111] Strategie kybernetické bezpečnosti USA z roku 2018. In unt.edu. [online]. [cit. 2023-02-14]. Dostupné z: https://digital.library.unt.edu/ark:/67531/metadc1259394/
[112] Národní centrum kybernetické bezpečnosti USA. In cyber-center.org [online]. [cit. 2023-02-14]. Dostupné z: https://cyber-center.org/
[113] National Institute of Standards and Technology. In nist.gov [online]. [cit. 2023-02-14]. Dostupné z: https://www.nist.gov/

kryptologická zpravodajská služba podřízena Ministerstvu obrany USA. NSA je odpovědná za sběr, analýzu a šíření zpravodajských informací a zajištění komunikační bezpečnosti USA. V rámci svých funkcí hraje NSA ze všech zpravodajských služeb USA důležitou úlohu při zajišťování obrany USA v kybernetickém prostoru.

Ostatní federální zpravodajské služby USA v tzv. zpravodajské komunitě USA (anglicky *U.S. Intelligence Community*)[114], kde působí dle dostupných informací 16 zpravodajských služeb, mají ve své působnosti jiné agendy. Nutno však dodat, že konečný počet známých zpravodajských služeb USA může být však mnohem větší a autor této práce pochopitelně nemusí vědět o některých zpravodajských služeb, které mají ve své agendě rovněž celý kyberprostor či pouze darknet, ale jejichž existence je veřejnosti utajovaná.

NSA má za úkol sledovat, analyzovat a odhalovat kybernetické hrozby a útoky proti americkým informačním systémům a sítím. Pro tento účel provádí širokou škálu kybernetických operací, které zahrnují sběr informací o kybernetických hrozbách, sledování kybernetických útoků a ochranu amerických sítí a systémů, a to často i preventivně s významným přesahem do zahraničí.

NSA má také za úkol vyvíjet a implementovat bezpečnostní protokoly a technologie jako např. šifrování dat za pomocí kryptografie, antivirovou ochranu nebo firewall, které významným způsobem přispívají ke zvýšení bezpečnostních zájmů USA před kybernetickými hrozbami.

Další úlohou NSA je spolupracovat s dalšími federálními prvky bezpečnostního systému USA, jakým jsou především ministerstvo obrany, ministerstvo vnitra, ministerstvo zahraničních věcí, prezident USA a ostatní zpravodajské služby USA, aby se koordinovala obrana USA v kybernetickém prostoru. NSA také spolupracuje s mezinárodními partnery v rámci NATO a velkým množstvím spojeneckých zpravodajských služeb.

[114] U.S. Intelligence Community. In intelligence.gov [online]. [cit. 2023-03-01]. Dostupné z: https://www.intelligence.gov/

4.4.2. Zpravodajské služby významné pro bezpečnostní zájmy USA

Veřejnosti jsou známé však i další zpravodajské služby vedle NSA, které mají různé specializace a úkoly:

- *Central Intelligence Agency* (zkratkou CIA) jako hlavní vnější ZS USA s poměrně výraznou historií a světovým věhlasem je zodpovědná za shromažďování, analýzu a poskytování zpravodajských informací na podporu americké zahraniční politiky. Jedním z jejich hlavních úkolů je provádění utajovaných operací v zahraničí, jako je například mapování, zadržování a případné zneškodnění teroristických organizací.
- *Federal Bureau of Investigation* (FBI) jako hlavní vnitřní ZS USA má ve své působnosti vyšetřování federálních zločinů, terorismu a protišpionážní činnosti na území Spojených států amerických.
- *National Geospatial-Intelligence Agency* (NGA) má své působnosti získávání, analýzu a poskytování zpravodajských informací oprávněným adresátům, které se týkají geografických a kosmických aspektů. NGA poskytuje důležité informace pro vojenské operace, humanitární zásahy a další oblasti.
- *National Reconnaissance Office* (NRO) má na starosti shromažďování informací z vesmíru a zajištění satelitního průzkumu pro potřeby zpravodajských služeb a vojenských operací ve vesmírném prostoru.
- *Defense Intelligence Agency* (americká DIA) je zodpovědná za shromažďování, analýzu a poskytování zpravodajských informací pro potřeby Ministerstva obrany USA a pro vojenské operace. DIA také spolupracuje s dalšími zpravodajskými službami a zahraničními partnery.[115]

[115] Defense Intelligence Agency. In dia.mil [online]. [cit. 2023-03-03]. Dostupné z: https://www.dia.mil/

CIA, NSA, americká DIA, NGA a NRO jsou považovány za tzv. “velkou pětku” (anglicky “big five”) hlavních amerických zpravodajských služeb.[116]

4.4.3. Recentní kybernetické útoky na USA

Mezi nejvýznamnější kybernetické útoky v USA patří útoky na vládní agentury, jako například útok na *Agenturu pro informační technologie a* v roce 2020, který pravděpodobně vedly ruské hackerské skupiny. Rovněž byly zaznamenány recentní útoky na soukromé společnosti a kritickou infrastrukturu, jako například útok na společnost SolarWinds, který umožnil útočníkům proniknout do sítí stovek firem a agentur.[117]

V současné době je kybernetická bezpečnost v USA stále předmětem zvýšené pozornosti a investic, s cílem posílit ochranu proti rostoucím hrozbám kybernetického prostoru. I přesto však zůstává kybernetická bezpečnost komplexním a neustále se vyvíjejícím problémem, který vyžaduje průběžné zlepšování a inovace.

4.5. NATO a jiné velmoci v oblasti kyberprostoru

Vztah Spojených států amerických jako vojenské a ekonomické supervelmoci 21. století a vojensky nejkompetentnějším členským státem NATO a Ruské federace jako státu, který je nejčastěji označován jako hackerská velmoc, je v kybernetickém prostoru napjatý.

Rusko je považováno mezi západními zeměmi za jednu z hlavních hrozeb v oblasti kybernetické bezpečnosti, a to zejména kvůli svému údajnému zapojení do mnoha útoků vůči západním zemím. V posledních letech se také zvýšil počet útoků v členských zemích Evropské unie i v USA, které jsou připisovány ruským státním aktérům.

Mezi nejvýznamnější kybernetické útoky, které byly připisovány Rusku v USA, patří například útok na demokratickou stranu během prezidentských voleb v USA

[116] Intelligence of USA. In informationweek.com. [online]. [cit. 2023-03-03]. Dostupné z: https://www.informationweek.com/leadership/intelligence-agencies-must-operate-more-like-an-enterprise

[117] SolarWinds explained. In techtarget.com. [online]. [cit. 2023-02-14]. Dostupné z: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

v roce 2016 (byť mediální přefouknutý, nebylo nikdy dokázáno, že tento útok byl veden z Ruské federace)[118], útok na elektrárnu v Ukrajině v roce 2015, útok na organizace pro kontrolu zbraní a další.

USA na tyto útoky reagovaly například rozšířením sankcí vůči ruským státním aktérům a zvýšením investic do své kybernetické obrany.

Nicméně je důležité poznamenat, že situace v kybernetické oblasti je velmi složitá a často se využívají techniky falešných vlajek a jiných triků, aby byly útoky připisovány jiným zemím. Proto není vždy jasné, kdo skutečně stojí za konkrétním kybernetickým útokem.

4.5.1. Možnosti dialogu s Ruskou federací

Ruská federace má rozvinutou kybernetickou infrastrukturu a aktuálně směřuje do této oblasti nemalé finanční prostředky, stejně jako do své armády (vzhledem ke svému celkovému HDP). Významným podílem se na obraně v kybernetické bezpečnosti Ruské federace podílí její zpravodajské služby, především Federální služba bezpečnosti (zkratkou FSB), která se zabývá bojem proti kybernetickému zločinu a ochranou kritické infrastruktury.[119]

Rusko se také aktivně zapojuje do kybernetických aktivit na mezinárodní úrovni, ať už v rámci vládních, vojenských nebo nevládních organizací. Ruské úřady a hackeři, který se nějakým způsobem hlásí k odkazu SSSR nebo Ruska, byli obviněni z mnoha kybernetických útoků, včetně útoků na zahraniční vlády, politické organizace, podniky a jednotlivce. Tyto útoky dle stanovisek zpravodajských služeb NATO často souvisejí s údajnou snahou Ruska o získání strategických informací a ovlivňování mezinárodního politického dění.[120]

Ruská federace a Česká republika jsou obě zeměmi s rozvinutými možnostmi obrany v oblasti kybernetického prostoru. Obě země mají vlastní strategie pro kybernetickou obranu a aktivně pracují na ochraně svých sítí a dat. Vztahy mezi

[118] Hacker attack 2016. In edition.cnn.com [online]. [cit. 2023-02-16]. Dostupné z: https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html
[119] Federal Security Service. In government.ru [online]. [cit. 2023-02-14]. Dostupné z: http://government.ru/en/department/113/
[120] Výroční zpráva BIS 2019-2021. In bis.cz [online]. [cit. 2023-02-16]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/

Ruskem a Českou republikou v oblasti kybernetické bezpečnosti jsou ovšem v posledních desetiletích problematické. V posledních letech se objevilo několik případů, kdy byly ruskými hackery napadnuty české instituce, včetně ministerstev, zpravodajských služeb a průmyslových podniků. Čeští představitelé obvinili následně ruské tajné služby z těchto útoků a vztahy mezi oběma zeměmi se kvůli nim výrazně ochladily, a to i přestože současný prezident ČR, Miloš Zeman, jehož mandát končí v březnu 2023, dlouhodobě usiloval o udržení přátelských nebo alespoň v oblasti hospodářství a obchodu diplomatických vztahů.[121]

Navzdory výše zmíněnému zhoršení vzájemných vztahů lze (nyní pouze v teoretické rovině) uvažovat o teoretickém prostoru pro spolupráci mezi Ruskem a Českou republikou v oblasti kybernetické bezpečnosti. Lze o tom uvažovat nicméně až poté, až bude současné vedení Ruské federace změněno, k čemuž dle názoru autor této práce dříve nebo později dojde. Obě země mají společné zájmy v boji proti kybernetickému zločinu a mohly by spolupracovat na ochraně kritické infrastruktury, jako jsou například jaderné elektrárny a telekomunikační sítě. Nicméně politické napětí vztahů mezi oběma zeměmi a situace na Ukrajině v posledních letech spolupráci ve všech myslitelných oblastech značně ztížilo.

Autor práce si dovolí vyjádřit názor, že Ruská federace (a především její současné vedení) by mohla být současným vývojem situace na Ukrajině a díky své současné geopolitické pozici donucena ukončit své ambice na obnovení úplného nebo částečného Svazu sovětských socialistických republik. Zároveň by dle názoru autora této práce měli nynější političtí představitelé Ruské federace přehodnotit svoje ambice o postavení supervelmoci, jakou byl SSSR vzhledem k tehdejším poměrům světových velmocí po druhé světové válce. SSSR bezpochyby byl v minulém století nejen vojenskou, ale i ekonomickou velmocí, nyní však jeho nástupnický stát, Ruská federace, již takovou pozici dlouhodobě nemá a nic zatím nenasvědčuje tomu, že by se na suverénní postavení SSSR po ekonomické stránce mohlo v nejbližší době vrátit. Ruská federace je totiž stále uznávaná jako vojenská velmoc, nicméně s velmi špatnou a v podstatě stagnující ekonomickou

[121] Russia behind cyber attack on Czech institutions. In radio.cz [online]. [cit. 2023-02-16]. Dostupné z: https://english.radio.cz/interior-minister-russia-behind-cyber-attack-czech-institutions-8748268

situací nemůže žádný stát světa stačit účinně reagovat na rychle se vyvíjející technologie a modernizace armád jiných velmocí, a to dlouhodobě ani v kybernetickém prostoru.

Dokonce si autor práce dovolí jít ještě dále a uvést názor, že mnoho nadbytečných problémů a sporů by mohlo být vyřešeno faktickým přijetím Ukrajiny, Ruské federace a případně i Běloruska mezi čekatelské nebo dokonce členské státy Severoatlantické aliance. Tímto krokem by se pravděpodobně otevřely problémy jiné, nicméně dle názoru autora práce by jich bylo stále méně.

Objektivně řečeno, otázka teoretického jednání o akceptování Ruské federace jako kandidátské země NATO je velmi kontroverzní a složitá. Autor práce uvede níže několik hlavních argumentů, které pojednávají pro i proti vstupu Ruska do NATO. Konečné rozhodnutí musí učinit političtí lídři Ruska, NATO a její členské země, zároveň nutno dodat fakt, že s přijetím by nemuselo souhlasit mnoho členských zemí NATO, tudíž by zde musela být autorita nebo situace, která všechny členské země NATO přesvědčí (což je v tento moment zcela vyloučené, ale lze hledět dle názoru autora práce i do budoucna, až skončí funkce současného prezidenta RF).

Dle článku 10 Washingtonské smlouvy, která je označována rovněž jako Severoatlantická smlouva, což je zakládající dokument NATO, je rozhodnutí o přijetí nového člena NATO přijímáno konsensem. Což znamená, že všechny členské státy musí souhlasit s přijetím nového člena, každý členský stát má tedy veto právo a může zabránit přijetí nového člena do NATO. Článek 10 uvádí (v překladu do českého jazyka): *"Smluvní strany mohou na základě jednomyslného souhlasu vyzvat kterýkoli jiný evropský stát, který je schopen napomáhat rozvoji zásad této smlouvy a přispět k bezpečnosti severoatlantického prostoru, aby přistoupil k této smlouvě. Každý takový smluvní stát se může stát smluvní stranou tím, že uloží u vlády Spojených států amerických svoji listinu o přistoupení. Vláda Spojených států amerických vyrozumí každou ze smluvních stran o uložení každé takové listiny o přistoupení."*[122]

[122] Washingtonská smlouva, čl. 10 a další. In natoaktual.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.natoaktual.cz/zpravy/lwashingtonskasmlouva

Rozšiřování NATO je navíc řízeno procesem, který je podroben určitým podmínkám a kritériím. Základní podmínky pro přijetí nového člena do NATO jsou následující:

A. Demokracie: Kandidátské země musí dodržovat základní principy demokratického právního státu.

B. Ekonomická stabilita: Kandidátské země by měly mít stabilní hospodářství a být schopny se účastnit aktivit NATO.

C. Bezpečnostní kritéria: Kandidátské země by měly být schopny plnit své závazky v oblasti obrany a bezpečnosti. To zahrnuje schopnost přijímat odpovědnost za vlastní bezpečnost a obranu, spolupráci se spojenci v oblasti obrany a schopnost přispět k obraně Aliance.

D. Geopolitická stabilita: Kandidátské země by měly být schopny stabilizovat své vztahy s okolními zeměmi a být schopny přispět k regionální stabilitě.

E. Kompatibilita: Kandidátské země by měly být schopny naplnit technické a vojenské standardy NATO, aby byly schopné spolupracovat se spojenci a zapojit se do společných operací.

Proces rozšiřování NATO probíhá postupně, kdy kandidátské země musí projít několika etapami, aby se staly členy. To zahrnuje podání žádosti o členství, splnění podmínek a kritérií a následně rozhodnutí Rady NATO o přijetí nového člena.

Lze také dodat, že Ruská federace zatím (což díky současné situace na Ukrajině se pravděpodobně ani nezmění, minimálně dokud bude v čele Ruské federace stále její současné vedení) ani nefiguruje v rámci politiky NATO o rozšiřování "Open Doors" mezi státy, o jejichž vstupu do NATO se dlouhodobě uvažuje.[123] Jsou jimi k datu 18. 2. 2023 Švédsko, Finsko, Gruzie, Ukrajina a Bosna a Hercegovina.

Lze zmínit několik argumentů pro čistě teoretické připuštění RF do NATO:

[123] NATO's Open Doors Policy. In nato.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato.int/docu/comm/1999/9904-wsh/pres-eng/04open.pdf

A. Bezpečnost: Vstupem Ruska do NATO by se posílila bezpečnost Evropy (České republiky nevyjímaje) a byla by vytvořena velká vojenská síla, která by mohla účinněji čelit společným hrozbám a výzvám. Třecí plochy jako jsou hranice s pobaltskými státy, Ukrajinou a dalšími zeměmi sousedními s NATO by jednom pro vždy byly eliminovány a neustálá obava o vlastní suverinitu, bezpečnost a o základní potřeby by pominula. Přijetím Ruské federace do NATO by se nečlenské státy, a to ani Čína, pravděpodobně neodvážily napadnout jakýkoliv členský stát NATO. Vnější nebezpečí státu Evropské unie by se tedy rapidně snížilo.

B. Spolupráce: Členstvím v NATO by se Rusko, které se řadí i v roce 2023 mezi vojensky nejmocnější státy světa,[124] stalo součástí jedné z nejvýznamnějších vojenských aliancí na světě a získalo by přístup k mnoha společným zdrojům, jako jsou informace, technologie a vojenské výcviky. Teoreticky toto platí i pro druhou stranu, kdy NATO by se mohlo od Ruska učit některé záležitosti a více se věnovat jiným záležitostem jako je například stále silnější postavení Čínské lidové republiky.

C. Ekonomické výhody: Vstupem do NATO by se mohla otevřít nová možnost pro hospodářskou spolupráci mezi Ruskem a členskými zeměmi NATO, což by mohlo vést k hospodářskému růstu a rozvoji. Rozhodně by obě strany mohly významně profitovat z obrovského nerostného bohatství.

Argumenty proti vstupu Ruska do NATO:

A. Rozpory: Mezi Ruskem a některými členskými zeměmi NATO existují značné politické spory, zejména v souvislosti s Ukrajinou a Gruzií. Tyto rozpory by mohly být dlouhodobou překážkou pro úspěšné fungování aliance.
B. Konfliktní situace: Ruská intervence v Ukrajině a podpora separatistických hnutí na východě Ukrajiny vyvolaly mezinárodní napětí a zpochybňují základní principy NATO, jako je ochrana územní integrity a suverenity členských zemí.

[124] The most powerful military in the world. In egscholars.com [online]. [cit. 2023-02-18]. Dostupné z: https://egscholars.com/2023/01/30/10-most-powerful-military-in-the-world-2022/

C. Nedostatek demokratického zřízení: Ruská federace je považována za nedemokratický režim, který příliš omezuje základní lidská práva a svobody a není dlouhodobě považována za demokratický právní stát. To by mohlo být překážkou pro vstup Ruska do NATO, která je založena na hodnotách demokracie a svobodného tržního hospodářství.

D. Rozdílné zájmy: Vzhledem k dlouhodobým postojům a náladám většiny obyvatel Ruské federace nelze vyloučit, že i když se změní vedení a proběhnou nezbytné reformy, aby Rusko splnilo základní podmínky k přistoupení do NATO, budou zde stále existovat imperiální ambice a zájmy většiny obyvatel Ruska. Ze současných průzkumů[125] totiž stále vyplývá, že většina občanů Ruské federace, ale také občanů jiných postsovětských republik, chápe rozpad SSSR jako ponížení a nejnešťastnější událost moderních dějin.[126] Nejen tedy současný prezident, Vladimir Vladimirovič Putin, ale i většina Rusů stále pociťuje určitý stesk a nostalgii po době největší slávy SSSR jako tehdejší supervelmoci světa. O této nostalgii bylo na internetu sepsáno poměrně velké množství článků (rusky *Ностальгия по СССР*). V posledních letech tyto nálady mezi obyvateli bývalého SSSR jsou dokonce na vzestupu.[127]

Autor práce si opět dovolí opakovat, že tato podkapitola pojednává spíše o stavu do budoucna, s tím, že v současné době je bližší dialog NATO s RF o jeho případném přistoupení mezi kandidátské země v podstatě vyloučený.

4.5.2. Vztah NATO s Čínskou lidovou republikou

Čínská lidová republika je již nyní považována za stejnou nebo v budoucnu i větší hrozbu v oblasti kybernetické bezpečnosti než RF. A to nejen kvůli údajnému zapojení čínských státních aktérů do mnoha útoků vůči západním zemím, ale také

[125] Nostalgia for the USSR (průzkum v ruštině). In levada.ru [online]. [cit. 2023-02-26]. Dostupné z: https://www.levada.ru/en/2017/12/25/nostalgia-for-the-ussr/
[126] Soviet nostalgia. In washingtonpost.com [online]. [cit. 2023-02-26]. Dostupné z: https://www.washingtonpost.com/news/worldviews/wp/2014/06/09/calls-for-a-return-to-stalingrad-name-test-the-limits-of-putins-soviet-nostalgia/
[127] 75 % občanů Ruské federace si myslím, že doba SSSR byla nejlepší v historii Ruska. In themoscowtimes.com. [online]. [cit. 2023-02-26]. Dostupné z: https://www.themoscowtimes.com/2020/03/24/75-of-russians-say-soviet-era-was-greatest-time-in-countrys-history-poll-a69735

kvůli vyšší konkurenceschopnosti a organizovanosti a koneckonců i mnohem rozsáhlejším lidským zdrojům.

V roce 2019 byla Čína poprvé zmíněna v závěrečném prohlášení Summitu NATO[128] jako hrozba pro alianci, zejména kvůli útokům na infrastrukturu a informační systémy západních zemí. NATO také uznalo, že Čína se stala hlavním hráčem v oblasti kybernetické bezpečnosti a vyslalo výzvu, aby se s tímto problémem vypořádala.

Čína na druhé straně tvrdí, že se snaží chránit své vlastní kybernetické systémy a bojovat proti kybernetické kriminalitě. Nicméně jsou stále hlášeny případy kybernetických útoků, které jsou připisovány aktérům působícím z teritoria Čínské lidové republiky.

Celkově je tedy vztah mezi NATO a Čínou v oblasti kybernetické bezpečnosti velmi složitý a napjatý, a je pravděpodobné, že se bude nadále vyvíjet v důsledku pokračujících útoků a konfliktů. Napětí přidalo i nedávné sestřelení čínského balónu armádou Spojených států amerických a Kanady, který bez povolení opakovaně narušoval teritoriální výsostné území obou států.[129]

Z hlediska předchozích kapitol o možnosti rozšiřování NATO uvádí autor této práce názor, že Čínská lidová republika se nikdy členským státem NATO nestane. Pokud by se tak stalo, smysl a účel NATO by se tímto krokem vytratil, jelikož by se NATO stávalo nadbytečnou vrstvou OSN, uvnitř které by se pravděpodobně následně vytvářely tlaky ze strany nesourodých a kulturně i ideologicky rozdílně nastavených členských států.

[128] Čína je vnímána jako hrozba pro NATO. In ceskatelevize.cz [online]. [cit. 2023-02-16]. Dostupné z: https://ct24.ceskatelevize.cz/svet/2994746-summit-nato-poprve-jako-moznou-hrozbu-vyslovne-zmini-cinu

[129] Čína protestovala proti sestřelení balonu. In cnn.com [online]. [cit. 2023-02-26]. Dostupné z: https://edition.cnn.com/2023/02/04/asia/beijing-reacts-us-jets-shoot-chinese-spy-balloon-intl-hnk/index.html

5. Možnosti zvýšení kybernetické bezpečnosti České republiky

Autor práce si dovolí níže shrnout některé stěžejní záležitosti, které by dle jeho názoru významně přispěly k zvýšení kybernetické bezpečnosti a uživatelské přívětivosti. V této kapitole autor práce nebude příliš odkazovat na další zdroje, jelikož to budou z velké části autorovy vlastní myšlenky.

5.1. Návrhy de constitutione et de lege ferenda

Česká republika by mohla přijmout několik legislativních kroků, které by pomohly zvýšit kybernetickou bezpečnost země:

A. Zavedení povinnosti hlášení kybernetických incidentů: Připravovaný nový zákon o kybernetické bezpečnosti, jehož pracovní verze je nyní představena široké veřejnosti k připomínkám[130] by mohl vymezit, co je považováno za kybernetický incident. Následně by všechny státní i soukromé organizace mohly lépe reagovat a plnit efektivně povinnost informovanost o všech těchto kybernetických incidentech, o kterých se dozví (a to i přestože by informování o některých incidentech mohlo být pro určité soukromé společnosti ekonomicky nevýhodné). Tato informace by mohla být následně předána NÚKIB a VZ, které by mohli mít sdílený informační systém pro tato hlášení s vysokým stupněm utajení.

   Nový zákon o kybernetické bezpečnosti ve své důvodové zprávě zmíní na základě dohody s NÚKIB aktuálně probíhající práce na migraci doménu ústředních orgánů státní správy na *.gov.cz, kterýžto záměr byl schválen vládou usnesením ze dne 11. ledna 2023 č. 23.[131] O protlačení podoby jednotné domény *.gov.cz přes prodloužené meziresortní připomínkové řízení a o schválení tohoto záměru vládou se významně zasadil autor této práce, který projekt od samého začátku vede na pracovní úrovni a koordinuje práci všech participujících subjektů.

B. Aktualizace a přesnější definice prvků a ochrany kritické infrastruktury: Krizový zákon a jeho prováděcí nařízení vlády č. 432/2010 Sb., o kritériích

[130] Nový zákon o kybernetické bezpečnosti možnost připomínkovat. In osveta.nukib.cz [online]. [cit. 2023-02-18]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145&fbclid=IwAR2Ft8zvQa-KJ1NiBePvFCc3PSxvcIV6EmRCqk29Ot1uZ4h7KrGc69Bh1Aw

[131] Usnesení vlády ze dne 11. ledna 2023 č. 23.

pro určení prvků kritické infrastruktury[132], který stanovuje minimální požadavky na kybernetickou bezpečnost pro kritickou infrastrukturu, včetně telekomunikačních sítí, elektroenergetických sítí, bankovních systémů a zdravotnických zařízení, by se měly novelizovat a významněji věnovat pozornost kyberprostoru a bezpečnostním zájmům ČR v této oblasti.

C. Zefektivnění práce s utajovanými informacemi: Aktuálně jsou standardy, metodiky a legislativa upravující práci s utajovanými informacemi dle názoru autora práce nemoderní. Administrativa spojená s touto činností způsobuje, že všichni aktéři se apriori snaží vyhnout jakémukoliv subsumování operace pod zařazení "tajné" nebo "přísně tajné", protože to průběh a efektivitu práce všech participujících subjektů značně ztěžuje.[133] Stává se tak, že běžní zaměstnanci ústředních správních úřadů bez bezpečnostní prověrky se při své práci často dostanou ne vlastním přičiněním a někdy i neúmyslně k dokumentům, ke kterým by se dostat neměli.
D. Zefektivnění vzdělávání a povědomí o kybernetické bezpečnosti prostřednictvím strukturálních změn právních předpisů a nastavení systému zejména středoškolského vzdělávání: Vzdělávací instituce by mohly přidat do svých výukových programů kurzy, ale i povinné nebo volitelné předměty přímo týkající se informačních technologií a kybernetické bezpečnosti. Větší důraz by se měl klást na základní a střední školy, aby se děti učily základním pravidlům kybernetické bezpečnosti a právu na digitální služby. Dle názoru autora práce by si však obecně vzdělávání v České republice zasloužilo mohutnou strukturální rekonstrukci.
E. Strukturálními změnami v oblasti vzdělávání by se mohly změnit i předpisy podporující materiálně obory, jichž je na trhu nedostatek. Tím by mohlo dojít k výraznému zvýšení počtu kybernetických expertů. Vláda by prostřednictvím finančních prostředků a změn systému vzdělávání mohla

[132] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury.
[133] Tento názor se postupně vyvíjel během informací získaných v rámci práce autora této diplomové práce na Úřadu vlády České republiky.

investovat do vzdělávání kybernetických odborníků, aby byl zvýšen počet lidí, kteří se v této oblasti specializují.

5.2. Koordinace bezpečnostních prvků bezpečnostního systému ČR

Jak již bylo pojednáno v kapitole druhé, Česká republika má mnoho institucionálních nástrojů, které se určitými způsoby podílí přímo na zajišťování kybernetické bezpečnosti státu nebo se podílí na souvisejících, příbuzných tématech, jako například digitalizaci státní správy nebo zajišťování obrany či informační bezpečnosti ČR.

Častým problémem, který způsobuje neúčinnou reakci na nastalé útoky je právě nevhodná, pomalá nebo neefektivní koordinace všech těchto institucionálních nástrojů, které jsou současně i bezpečnostními prvky bezpečnostního systému České republiky. Autor práce tak již ve své předchozí diplomové práci, která se věnovala kontrole zpravodajských služeb s názvem *"Zpravodajské služby a kontrola jejich činnosti se zaměřením na Českou republiku"* zmiňoval, že tento problém by mohlo částečně vyřešit zřízení monokratického orgánu po vzoru Izraele a USA, tzv. Poradce pro národní bezpečnost.

Jako protiargument, který zaznívá často i od některých krizových manažerů, s nimiž měl možnost autor práce toto téma diskutovat, zněl, že již tu přece máme výbory Bezpečnostní rady státy, zejména pak výbor pro kybernetickou bezpečnost, výbor pro zpravodajskou činnosti, výbor pro obranné plánování nebo výbor pro vnitřní bezpečnost.[134]

Tyto výbory však nejsou monokratické, naopak má v nich zastoupení poměrně velké množství bezpečnostních státních organizací a jejich svolávání a fungování probíhá zřejmě zhruba stejně efektivně jako svolávání a koordinace jiných pracovních skupin a výborů ve státní správě. Z tohoto důvodu si dovolí autor práce uvést názor, že by měly být buď nahrazeny nebo doplněny právě zmíněným monokratickým orgánem, který bude schopen pružně reagovat na nastalé hrozby a krizové situace.

[134] Výbory Bezpečnostní rady státu. In mvcr.cz [online]. [cit. 2023-02-22]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-rada-statu-brs.aspx

Jak totiž z výše uvedeného vyplývá, během vlastního řešení krizových situací a nastalých hrozeb, které je třeba v zájmu zajišťování bezpečnostních zájmů České republiky vyřešit, v co nejkratším časovém intervalu, není čas na zdlouhavé demokratické procesy a diskutování.

Autor práce uvede na poněkud nevšedním příkladu, proč monokratický orgán bude ve většině případů vhodnější pro řízení zvládnutí krizových situací.

V dobách, kdy se z římské republiky stával v té době nejsilnější stát antického světa, znalo římské právo institut tzv. diktátora (latinsky *dictator*: *"ten, který přikazuje"*), titulován také latinsky *magister populi* („velitel lidu"), *praetor maximus* („nejvyšší praetor") nebo *magister peditum* („velitel pěchoty"). Tento mimořádný politický monokratický orgán byl ustaven římským senátem v době složitých bezpečnostních nebo vojenských okolností na omezenou dobu půl roku, s možným prodloužením. Na tento orgán se jako na jediný v dobách římské republiky právě nevztahovaly principy římského práva jako zásada annuity, podle níž výkon funkce je přípustný po dobu jednoho roku, zásada kolegiality, podle níž jsou řízeny úřady prostřednictvím většího množství osob, nebo zásada odpovědnosti, která stanoví nemožnost stíhat za činy spáchané v době vykonávání úřadu.[135]

Antičtí Římané zřídili tento úřad devět let po svržení Římského království vyhnáním posledního římského krále Targuinia Superba v roce 510 př. n. letopočtem. Věděli již za republiky, že přestože respektují principy, že si jedinci nemohou uzurpovat moc pro sebe, zásada kolegiality není efektivní, ani moudrá při řešení náhlých nebo bezprecedentních bezpečnostních hrozeb celého státu (jako jsou válečné konflikty, vnitřní nepokoje narušující chod státu, konání velkých her, v období bouřlivých voleb atp.).

Autor této práce si je vědom, že tehdejší podmínky a úroveň poznání nejsou srovnatelné se současnými, nicméně určitá logika v tomto uspořádání monokratického orgánu v podobě koordinátora, vedoucího nebo v podobě poradního orgánu během krizových situací tu je dle názoru autora práce zřetelná.

[135] SKŘEJPEK Michal, KINCL Jaromír, URFUS Valentin. Římské právo, vydání 1.. Nakladatelství C. H. Beck. Datum vydání 1995. počet stran 408. ISBN: 80-7179-031-1.

Jako další příklad podporující efektivitu monokratického orgánu jsou samozřejmě již zmínění poradci pro národní bezpečnost USA a Izraele nebo již zmíněný inspektor pro kybernetickou obranu.

5.3. Přeměny některých organizacích

Autor práce v této podkapitole uvede několik důvodů, proč by sloučení (kromě SZR a některých digitalizačních odborů MV) v této práci zmiňovaných ústředních orgánů státní správy zaměřených na IT nebo kybernetickou bezpečnost, mohlo být výhodné.

Autor práce si je vědom toho, že k tomu pravděpodobně výhledově v rámci desítek let nedojde, protože se vlády většinou bojí provádět větší institucionální či legislativní řezy, což je dle názoru autora práce škoda. Nicméně i tak to je dle názoru autora práce relevantní myšlenka, která může být do jisté míry inspirativní i z hlediska odstraňování resortismu a zvýšení horizontální i případné vertikální spolupráce státních organizací v souvislosti s možnou novelizací zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

Zároveň autor práce uvádí, že k případnému sloučení NÚKIB a DIA a případných dalších organizací zaměřených na IT nebo kybernetickou bezpečnost by mohlo dojít různými způsoby, přičemž jedním ze způsobů by bylo přenesení veškerých agend z jednoho úřadu na druhý a faktická redukce již dnes velkého počtu ústředních orgánů státní správy. Čistě z jazykového hlediska by, pokud by se neuvažovalo o změně názvu, byl vhodnějším názvem pro výchozí organizaci zřejmě stávající název Digitální a informační agentury.

Zde jsou některé důvody, které by dle názoru autora práce mohly podpořit sloučení DIA a NÚKIB:

- Synergie mezi digitalizací a kybernetickou bezpečností: Digitalizace přináší nové výzvy v oblasti kybernetické bezpečnosti, a to zejména kvůli zvyšování množství dat a aplikací, které jsou digitálně přístupné. Přenesením agendy kybernetické bezpečnosti na DIA by bylo možné lépe koordinovat digitalizační projekty a zároveň zajistit jejich bezpečnostní aspekty.

- Větší efektivita a úspora nákladů: Převedení agendy kybernetické bezpečnosti z NÚKIB na DIA by mohlo přinést větší efektivitu a úsporu nákladů. DIA by mohla využít své stávající kompetence a infrastrukturu v oblasti digitalizace a zároveň snížit náklady na správu dvou oddělených orgánů.
- Lepší koordinace a větší pružnost: NÚKIB se zaměřuje na širší spektrum úkolů v oblasti kybernetické a informační bezpečnosti, zatímco DIA se soustředí na digitalizaci a modernizaci veřejné správy. Přenesení agendy kybernetické bezpečnosti na DIA by mohlo vést k lepší koordinaci a větší pružnosti při řešení konkrétních výzev a hrozeb v oblasti kybernetické bezpečnosti.
- Inspirace již několikrát zmíněnou, zkušenější a úspěšnou Estonským úřadem pro informační systémy, který koncentruje kybernetickou bezpečnost i digitální agendy, (zkratkou RIA), který funguje dle mezinárodních komparací velmi dobře.

Je třeba podotknout, že sloučením obou existujících ústředních správních úřadů by vyžadovalo nejen silnou politickou vůli vlády, ale i dobrou spolupráci mezi zejména vedoucími zaměstnanci DIA a NÚKIB, aby bylo zajištěno, že budou plně pokryty všechny aspekty kybernetické bezpečnosti a aby byly zachovány všechny základní principy ochrany kritické infrastruktury a bezpečnostních zájmů ČR.

Autor práce si v tomto kontextu dovolí zmínit, že i přechod některých odborů Ministerstva vnitra České republiky na Digitální a informační agenturu nebyl zcela hladký, a přestože na první pohled by se to nemuselo zdát jako náročné, ve skutečnosti je s tím více administrativní práce (díky dle názoru autora práce velmi rigidním právní úpravě ČR), než by si kdy kdo dokázal představit.

Zároveň autor práce dodává, že by v této souvislosti některé mohlo napadnout i čistě teoretické sloučení DIA, NÚKIB nebo jednoho z těchto ústředních správních úřadů s NCKO nebo případně i celým Vojenským zpravodajství. Takový krok by ale dle názoru autora práce byl již nejen neefektivní, mimořádně administrativně náročný, ale také nelogický a bezpečnostní zájmy České republiky ohrožující.

VZ jako zpravodajská služba pod Ministerstvem obrany ČR, jehož příslušníci jsou ve většině vojáci z povolání, je specifickou státní organizací, u které by slučování s některým z ÚSÚ z podstaty věci nebylo v Českém prostředí možné, i kdyby to mělo znamenat teoretickou vyšší míru informovanosti a spolupráce zaměstnanců NÚKIB, DIA a VZ.

Případné sloučení NÚKIB, DIA a VZ by navíc mohlo vést k tomu, že by se tím teoreticky vytvořila obrovská zpravodajská služba s vlastním rozpočtem v teoretickém postavení ústředního orgánu státní správy, což je v Českém prostředí mimo jakoukoliv oblast úvah.

5.4. Preventivní opatření k Metaverse

S přechodem do virtuálního prostředí Metaverse mohou být zájmy lidské bytosti a citlivé osobní i utajované informace vystaveny řadě nových rizik a hrozeb. Zde jsou několik z nich:

- Kybernetické útoky: S virtuální realitou Metaverse vznikají nové cesty, jak mohou útočníci proniknout do sítí a získávat citlivé osobní i utajované informace. Hrozby zahrnují phishing, ransomware, malware a další formy útoků, které jsou zaměřeny na uživatele virtuální reality a platformy Metaverse.
- Identita a soukromí: V Metaverse je možné vytvořit různé identity a uživatelské účty, což může vést k riziku identity theft. Uživatelé také sdílejí osobní údaje a data, která mohou být ohrožena v případě kybernetických útoků nebo zneužití.
- Virtuální zločin: Metaverse může vytvořit nové prostředí pro virtuální zločiny, jako jsou například podvody, krádeže a další formy trestné činnosti.

Česká republiky a případné jiné členské státy Evropské unie by měly přijmout několik opatření, aby ochránily své bezpečnostní zájmy v Metaverse:

A. Legislativa: Státy by měly přijmout legislativní rámec a právní předpisy upravující kybernetickou bezpečnost a ochranu osobních údajů v Metaverse. Tyto zákony by měly být navrženy v obecnějším a pružnějším duchu tak, aby se přizpůsobily rychle rozvíjejícímu se virtuálnímu prostředí,

a nemuseli se tak političtí představitelé ČR bránit novým inovacím. Měly by také jasně definovat všechny termíny a pojmy, která se běžně používá v prostředí vývoje virtuálních prostředí a sjednotit tak terminologii.

B. Ochrana před kybernetickými útoky: Státy by měly investovat do ochrany svých sítí a infrastruktury před kybernetickými útoky a zajistit, aby poskytovatelé a správci virtuálního prostředí dodržovali standardy kybernetické bezpečnosti.

C. Zvyšování povědomí: Státy by měly pomáhat uživatelům Metaverse zvyšovat povědomí o kybernetických hrozbách a naučit je, jak se chránit před riziky, jako jsou phishing, malware, podvodné praktiky popsané v kapitole 1.5 této práce a jiné formy kybernetických útoků.

D. Spolupráce mezi státy: Vzhledem k tomu, že virtuální realita Metaverse není nijak omezena žádnými hranicemi, je důležité, aby státy spolupracovaly na mezinárodní úrovni a vyměňovaly si informace a osvědčené postupy v oblasti kybernetické bezpečnosti a ochrany osobních údajů. V nejlepší případě by mohla být stěžejní právní úprava na mezinárodní úrovni nebo alespoň na úrovni Evropské unii harmonizovaná nebo přímo sjednocená.

5.5. Sjednocení domén státních institucí na *.gov.cz

Autor této práce si dovolí zmínit jako další stěžejní příležitost zvýšení kybernetické bezpečnosti i velmi aktuální projekt migrace na jednotnou doménu *.gov.cz a vytvoření jednotného vizuálního stylu ústředních orgánů státní správy. Tento projekt má tu čest jménem místopředsedy vlády pro digitalizaci a jménem jeho náměstků na pracovní úrovni vést a koordinovat činnost všech spolupracujících subjektů státní správy (zejména NÚKIB, MV ČR Odbor eGovernmentu a Odbor Hlavního architekta eGovernmentu, MZV a CZ.NIC).

Tyto dva schválené záměry jsou stejně jako vytváření Digitální a informační agentury velmi čerstvé záležitosti a v průběhu psaní této diplomové práce probíhají práce, které realizaci migrace na *.gov.cz posunují dále.

V dobrém progresu je i zavádění jednotného Design systému (https://designsystem.gov.cz/#/) státní správy, na jehož propagaci se autor této práce rovněž významně podílel. Například 2. března vedl společně s kolegy z Odboru eGovernmentu školení zástupců všech ústředních orgánů státní správy v budově Strakovy akademie na Úřadu vlády České republiky.

Projekt byl spuštěn na podzim 2022, kdy autor této práce zahájil v přípravné fázi jednání se všem resorty a přípravu materiálu ke schválení vládou.

Jak je vidno z elektronické knihovny právních předpisů, v prodlouženém meziresortním připomínkovém řízení přišlo od různých připomínkových míst na 90 konstruktivních a dobrých připomínek, které se nakonec podařilo všechny vypořádat, zejména s pomocí některých kvalifikovaných lidských zdrojů NÚKIB, CZ.NIC a tehdejších zaměstnanců odborů MV, které k 1. dubnu 2023 přecházejí pod DIA. Vládě tak byly záměry migrace na jednotnou doménu a vytvoření jednotného vizuálního stylu ústředních orgánů státní správy předloženy bez rozporů a vláda oba záměry schválila. Autor práce je od podzimu 2022 v úzkém kontaktu a kooperaci s mnoha kvalifikovanými lidskými zdroji, především z NÚKIB, a některých odborů MV (budoucími zaměstnanci DIA), ZS ČR, MMR, MZV a dalšími. Spolupráce těchto akterů je zcela nezbytná, aby projekt byl dotažen do zdárného konce.

Níže si dovolí autor práce, autor myšlenky celého postupu projektu a autor již schváleného usnesení vlády ze dne 11. ledna 2023 č. 23, Mgr. Bc. Michal Daněk, projekt migrace na jednotnou doménu *.gov.cz přiblížit a uvést některé zásadní argumenty na podporu tohoto projektu. Některé argumenty byly autorem této práce použity i během obhajoby projektu a jako podklad pro místopředsedu vlády pro digitalizaci k jednání vlády. V žádném případě autor práce nekopíruje texty jiných autorů nebo jiných organizací, všechny níže uvedené myšlenky a argumenty jsou vlastní argumenty autora vytvořené autorem této práce.

Webové i e-mailové domény ústředních orgánů státní správy a jejich zřizovaných organizací v současné době obsahují různé, nekoordinovaně vybrané, české nebo cizojazyčně zkratky organizací či celá slova nebo různou změť písmen, ze které

běžnému uživateli často nemůže být srozumitelné, že se jedná o web či pracovní e-mail státní instituce, a ne o digitální produkt soukromé společnosti či dokonce o internetovou stránku podvodné entity. Příkladem nesjednocenosti domén ústředních správních úřadu[136] explicitně jmenovaných v zákoně č. 2/1969 Sb., kompetenčním zákoně, budiž: *eagri.cz*, *mkcr.cz*, *czso.cz*, *vlada.cz*, *justice.cz* nebo *army.cz.*

NÚKIB ani jiná státní autorita nemá přehled o všech používaných doménách. Není tak možné efektivně skenovat zranitelnost systémů na doménách, které jsou dostupné koncovým uživatelům (klientům státní správy) v prostředí internetu. Kvůli nejednotnosti domén není také možné centrálně nastavovat technická pravidla a zajistit bezpečnost celého řetězce DNS záznamů. V současné době si každý správce systému řeší bezpečnost DNS dle svého uvážení, a vynucovat jednotná pravidla fungování pouze formou standardů je nedostatečné.

V některých případech jsou doménová jména dokonce registrována na fyzické osoby, a není tak možné ani pro NÚKIB ani pro běžné uživatele ověřit legitimnost domény. Klienti státní správy tak dnes vzhledem k často ospravedlnitelné nemožnosti identifikace zkratky či slova ze znění odkazu nemají dostatečnou jistotu, že pod určitým linkem se ocitnou skutečně na webu státní instituce. To otevírá možnosti pro podvodné techniky, jakým byl například nedávný phishing útok přicházející z podvržené domény „*mpsv-cz.cz“*.[137] V návaznosti na informace o uvedeném phishing útoku na MPSV jsou zaznamenané případy napodobování nejen domén webových stránek státních institucí, ale i jejich vizuální styl, respektive jejich často se měnící a nesjednocený design, čehož podvodníci rovněž zneužívají a snadno tak zkopírují např. Portál občana, vytvoří snadno odkazy na sofistikovaný falešný napodobený web. Díky tomu, že státní instituce používají změň různých svých designů, nemohou mít občané šanci si zvyknout na určitou

[136] Zákon č. 2/1969 Sb., kompetenční zákon. § 1 a § 2.
[137] Phishing útoky na MPSV. In mpsv.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.mpsv.cz/-/falesne-domeny-napodobuji-web-mpsv-jde-o-phishing-stranky-jsou-jiz-zablokovany

podobu a standard digitálních produktů státní správy, s kterými by mohli trvale počítat.[138]

Situace v případě e-mailových domén státních zaměstnanců je rovněž nevyhovující. Na každém ústředním správním úřadě je metodika mailových adres odlišná a často i matoucí, v některých případech je pracovní e-mail psán nejdříve příjmení, pak jméno, někdy chybí i jméno, někde se píše mezi příjmení a jméno podtržítko, jindy tečka. Níže autor práce uvede příklady:

- Úřad vlády České republiky: prijmeni.jmeno@vlada.cz
- Ministerstvo zahraničních věcí: jmeno_prijmeni@mzv.cz
- Ministerstvo průmyslu a obchodu: prijmeni@mpo.cz
- Ministerstvo práce a sociálních věcí: jmeno.prijmeni@mpsv.cz
- Správa státní hmotných rezerv: grpsek-predseda@sshr.cz
- Úřad průmyslového vlastnictví: (x znamená v tomto případě počáteční písmeno jména): xprijmeni@upv.gov.cz
- Rada pro rozhlasové a televizní vysílání: prijmeni.x@rrtv.cz (tedy obráceně)
- Národní sportovní agentura: prijmeni@agenturasport.cz

Aktuálně preferovaná varianta sjednocených pracovních i služebních e-mailových adres všech státních zaměstnanců státní správy je: jmeno.prijmeni@dia.gov.cz (dia jako příklad zkratky ústředního orgánu státní správy). V případě více zaměstnanců se shodným jménem a příjmení se preferuje psát před @ číslici a v případě více jmen a příjmení se zatím preferuje možnost zmiňovat pouze jedno hlavní používané nebo zaměstnancem preferované jméno a jedno hlavní používané nebo zaměstnancem preferované příjmení.

Již před 20 lety, konkrétně v roce 2002, se pokusil o sjednocení všech domén státní správy pod doménu 1. a 2. řádu *.gov.cz tehdejší Úřad pro státní informační

[138]Zneužívání falešného webu Portálu občana. In antivirovecentrum.cz [online]. [cit. 2023-03-11]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/podvodnici-zneuzivaji-falesny-portal-obcana.aspx

systém.[139] Pozdějším začleněním tohoto úřadu do Ministerstva informatiky v roce 2006 vydalo tehdejší Ministerstvo informatiky pro orgány veřejné moci metodický pokyn pro tvorbu a přidělování domén třetí úrovně pod jednotnou doménou 1. a 2. řádu ve formě **.gov.cz*.[140] Nejčastěji zmiňovaná varianta jednotné domény je to i dnes, a některé organizace, jako například Úřad průmyslového vlastnictví (https://upv.gov.cz/) nebo Státní zemědělská a potravinářská inspekce (https://szpi.gov.cz/) již tuto podobu jednotné domény implementovaly. Gov.cz používá také stěžejní personalizované místo pro poskytování služeb eGovernmentu, Portál občana (https://portal.gov.cz/), rozpracovaný design systém pro internetové stránky a mobilní aplikace státních organizací (https://designsystem.gov.cz) nebo ad hoc zřízené webové stránky jako např. (https://covid.gov.cz/). Internetová stránka gov.cz (https://gov.cz/) slouží, podobně jako v případě Estonska gov.ee, již nyní jako přehledný rozcestník některých služeb veřejné správy , který mimo jiné již zároveň implementoval grafické prvky designsystem.gov.cz. Je zřejmé, že zvolením jiné varianty, než je *.gov.cz by docházelo již v tento okamžik k nadbytečnému zmatení v mezičase zavedení a k nadbytečným nákladům při opětovné migraci.

Doména gov.* je navíc zažitá v mnoha státech s vyspělou kulturou digitalizace státní správy. Tato doména je běžnou praxí v mnoha zemích Severoatlantické aliance a v téměř polovině zemí Evropské unie, jako příklad lze uvést Velkou Británii, Austrálii, Belgii, Chorvatsko, Maďarsko, Slovinsko, Estonsko nebo Polsko. Zároveň její velkou výhodou je univerzální funkčnost napříč světovými jazyky. Při komunikaci zahraničních partnerů s tuzemskými úřady nedochází k žádným pochybnostem, že jde o vládní instituci. Varianty **.cesko, *.stat.cz* nebo **.vlada.cz*, kterou nyní používá Úřad vlády ČR, by pro zahraniční partnery a pro spojenecké státy Severoatlantické aliance mohly být v mnoha případech nesrozumitelné a v praktické rovině by mohly negativně ovlivňovat například činnost institucí zaměřených na zahraniční obchod a podporu exportu.

[139] Informační systémy ve veřejné správy. In homel.vsb.cz, 2011. [online]. [cit. 2022-11-14]. Dostupné z: https://homel.vsb.cz/~dan11/is_skripta/IS%202011%20-%20IS%20ve%20statni%20sprave.pdf

[140] Doménová revoluce. In lupa.cz, 2002. [online]. [cit. 2022-11-14]. Dostupné z: https://www.lupa.cz/clanky/domenova-revoluce-ve-verejne-sprave/

V návaznosti na hackerské útoky a vůli posílit kybernetickou bezpečnost ústředních správních úřadů ČR uložila Bezpečnostní rada státu NÚKIB svým usnesením ze dne 12. dubna 2022 č. 15[141] rozpracovat projekt BIVOJ, v jehož rámci figuruje již dlouhodobě návrh sjednocující domény **.gov.cz*. Z výstupů pracovních schůzí tohoto projektu vyplynulo, že na jednotné doméně panuje vzhledem k výše zmíněným důvodům shoda na úrovni do přípravy projektu zapojených ústředních bezpečnostních složek bezpečnostního systému České republiky, přičemž pro úplnost uvádíme, že ale nejde o všechny bezpečnostní složky.

Tento záměr, který cílí v první fázi na zpracování harmonogramu před následnou migrací webových domén a emailových, respektive poštovních domén všech ústředních orgánů státní správy a státní institucí, které se rozhodnou do migrace svých domén zapojit dobrovolně, byl schválen vládou 11. 1. 2023 usnesením č. 23.

Během migrace by nemělo být přistoupeno dle názoru autora této práce k centrální distribuci TLS/SSL certifikátů. Podrobnosti týkající se certifikátů a jiných dílčích technických záležitostí budou detailněji zpracovány v auditu a harmonogramu, který se ukládá návrhem usnesení vlády vypracovat.

Dle názoru autora této práce by se měly původní domény zachovat alespoň po dobu dalších 10. let, kdy budou schopné redirektovat případné uživatele veřejné správy přes stávající (starou) doménu na oficiální doménu novou. V zájmu zvyšování kybernetické bezpečnosti a UX uživatelů státní správy, což je obecně účelem tohoto projektu, budou muset některé dlouhodobě zažité domény (jako např. policie.cz) zůstat ve vlastnictví České republiky.

Záměr migrace domén na sjednocenou doménu 1. a 2. řádu *.gov.cz ústředních orgánů státní správy, který vláda svým usnesením ze dne 11. ledna 2023 schválila[142], by měl cílit pouze na tzv. viditelné domény v zájmu zvyšování UX, nikoliv na změny domén v uzavřené síti CMS/KIVS dle zákona č. 365/2000 Sb., o

[141] Usnesení vlády ze dne 12. dubna 2022 č. 15.
[142] Usnesení vlády ze dne 11. ledna 2023 č. 23.

informačních systémech veřejné správy[143], ve znění pozdějších předpisů, kde platí pro DNS jiná pravidla a kde každá organizace musí zajistit, že DNS jsou jiné pro koncové uživatele v internetu a jiné pro vnitřní komunikaci státu v CMS/KIVS .

[143] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.

Závěr

Přiznané pravomoci Vojenskému zpravodajství v oblasti zajišťování obrany státu v kybernetickém prostoru představují porušení určitých zásad zpravodajských služeb České republiky. VZ může kromě běžných zpravodajských agend nově přímo reagovat v nutných případech na hrozby v kybernetickém prostoru. Vzhledem k obávám do přílišného zasahování VZ do základních práv a svobod má poměrně velkou zodpovědnost. Z toho vyplývá i potřeba zvýšené kontrola jeho činnosti. Nad rámec stávajících kontrolních mechanismů českých zpravodajských služeb tak nově činnost VZ kontroluje i k tomu zřízený monokratický orgán, inspektor pro kybernetickou obranu. Tento orgán nicméně naráží dle názoru autora práce na určité limity své nezávislosti, když je sice podřízen přímo ministryni obrany, ale stále příslušníkem VZ.

Jako další relevantní monokratický orgán byl zřízen i tzv. Poradce pro národní bezpečnost. Již jmenovaný Poradce pro národní bezpečnost by měl výrazně pomoci koordinovat komunikace klíčových bezpečnostních prvků během řešení krizových situací a zajišťování bezpečnostních zájmů České republiky.

Česká republika zaostává dle některých mezinárodních indexů ve srovnání s jinými státy Evropské unie v oblasti digitalizace státní správy i v oblasti zajišťování kybernetické bezpečnosti. Je zde poměrně velký prostor pro zefektivnění zmíněných měřených oblastí v několika úrovních:

- na úrovni právní úpravy, tedy legislativní,
- na úrovni institucionální a koordinační,
- na úrovni technické, s níž je spjat i dostatek kvalifikovaných lidských zdrojů a
- na úrovni vzdělávání a šíření povědomí o IT a kybernetické bezpečnosti nejen mezi úředníky, ale i mezi občany.

Pro úplnost ale lze zmínit, že existují indexy kybernetické bezpečnosti jako např. tzv. National cyber security index (zkratkou NCSI) dle kterých se Česká republika umisťuje zejména díky velmi dobré práci zaměstnanců zmiňovaného NÚKIB v posledních letech velmi dobrých pozicích ze všech zemí světa, dle NCSI dokonce na 5. místě. Což je vynikající hodnocení, jednu příčku za Estonskem a před

skandinávskými státy, před Německem nebo před USA, které zase obsazují dle jiných indexů první místo.[144] Tato mezinárodní srovnávání a hodnocení všech států světa je třeba brát tedy s velkou rezervou, jelikož z podstaty věci nelze aktualizovaně kvalifikovaně sbírat, analyzovat a vyhodnocovat všechna kvalifikovaná data současně ze všech států světa, když se situace v kybernetickém prostoru dynamicky neustále vyvíjí.

Možnosti zefektivnění těchto čtyřech úrovních je podrobněji rozepsáno v kapitolách 2., 4. a zejména kapitole páté. Česká republika se v mnohém může inspirovat dle názoru autora práce od Estonska, Izraele nebo Dánska.

Finanční zdroje by Česká republika měla dle názoru autora práce k dispozici (například z Národního plánu obnovy, kde je kybernetické bezpečnosti věnována celá jedna kapitola 1.2.)[145], Česká republika je však nedokáže efektivně čerpat.[146] Tomu by mělo již v tomto roce výrazně pomoci nadresortní a efektivní řízení digitalizačních agend nové Digitální a informační agentury a restrukturalizace Rady vlády pro informační společnost na Úřadu vlády ČR, o kterézto strukturách tato práce také pojednává.

Některé možnosti zvýšení či zefektivnění kybernetické obranyschopnosti státu jsou podrobně rozepsány v kapitole páté. Autor práce v tomto ohledu uvádí, že na projektech sjednocení domén na *.gov.cz a zavádění design systému webových stránek ústředních správních úřadů odvedl velký kus práce a na pracovní úrovni tento projekt v době psaní této práce vede a koordinuje činnost všech participujících orgánů. Ve struktuře RVIS pod výborem pro informační koncepci České republiky vznikne 17. března 2023 na toto konto i oficiální pracovní skupina, které bude autor této práce předsedat. Argumenty, které jsou uvedeny v této práce tedy jsou vlastní rešerší autora, která probíhala na podzim minulého roku, v kterézto době autor práce *záměr migrace na jednotnou doménu *.gov.cz a vytvoření jednotného vizuálního stylu ústředních orgánů státní správy* připravil. V

[144] Hodnocení všech států světa v kybernetické bezpečnosti. In ncsi.ega.ee [online]. [cit. 2023-03-11]. Dostupné zhttps://ncsi.ega.ee/ncsi-index/?order=rank
[145] Digitální transformace, kapitola 1.2 v Národním plánu obnovy. In planobnovy.cz, 2023. [online]. [cit. 2023-02-26]. Dostupné z: https://www.planobnovycr.cz/digitalni-transformace-3
[146] Závažné nedostatky čerpání z evropských grantů. In ekonomickydenik.cz, 2023. [online]. [cit. 2023-02-26]. Dostupné z: https://ekonomickydenik.cz/ceska-republika-muze-prijit-o-miliardy-z-evropskych-grantu-inventura-mpo-zjistila-zavazne-nedostatky/

rámci své práce na v Odboru kabinetu místopředsedy vlády pro digitalizaci se věnoval i práci zakládání Digitální a informační agentury. Autor práce psal například značnou část obecné části důvodové zprávy k dnes již z části účinného a platného zákona č. 471/2022 Sb., o změně digitální ústavy a některých dalších zákonů. Z tohoto důvodu jsou některé informace a texty o DIA v této práci přímo dílem autora samotného.

Autor práce se rovněž poměrně významně věnoval problematice aktuálního často skloňovaného tématu Metaversa, tedy virtuálních světů a umělé inteligence. Lze očekávat, že by se sem mohly přesouvat některé oblasti života některých jedinců či skupin obyvatel, kteří z různých důvodů nemusí být šťastni v reálném, fyzickém světě (je možné, že by se to mohlo týkat i zdravotně postižených osob). Do těchto virtuálních světů se budou společně s případnými občany ČR přesouvat i bezpečnostní zájmy České republiky.

Z tohoto důvodu zejména je nutné, aby byly bezpečnostní složky včas připravené reagovat na hrozby, které se mohou ve virtuálních světech objevovat. Kromě krádeže identity, finančních a majetkových zdrojů nebo autorství toho, co by mohlo být ve virtuálních světech vytvořeno, lze uvažovat téměř o všech myslitelných lidských právech a svobodách, které by mohly být ve virtuálních světech v budoucnu ohrožovány. Byť to může být otázka budoucnosti, musí se myslet preventivně na všechny rizika a hrozby, které jsou v některých případech i popisovány ve vědeckých, futuristických či satirických dokumentech jako například některé epizody seriálu Black Mirror.

Díky tomu, že přiznání pravomocí Vojenskému zpravodajství je stále ještě čerstvá záležitost a díky tomu, že například funkce inspektora pro kybernetickou obranu byla obsazena teprve před několika málo měsíci, podílí se na zajišťování kybernetické bezpečnosti státních institucí, včetně obrany státu v kybernetickém prostoru do stále ještě rozhodující míry NÚKIB, který je stále vládním CERT České republiky.

Je to stále také NÚKIB, o kterém je slyšet v souvislosti s kybernetickou bezpečností státu v tuzemsku i v mezinárodním společenství, a je to stále NÚKIB,

na kterého se občané i státní zaměstnanci obrací v souvislosti s kybernetickou bezpečností.

O VZ a jeho úloze v oblasti obrany státu v kybernetickém prostoru bude ale dle názoru autora této práce v budoucnu díky vytvoření NCKO větší povědomí.

Lze říci, že bezpečnostní systém České republiky je v době psaní diplomové práce díky mnoha nástrojům vlády a členité struktuře bezpečnostních systému ČR (a nyní i díky nově vzniklé koordinační funkci Poradce pro národní bezpečnost, o kterém autor práce pojednal ve více kapitolách) způsobilý k zajišťování obrany České republiky. Aby však Česká republika byla schopna efektivně, včas a důsledně reagovat na všechny kybernetické hrozby a rychle tempo vývoje informačních technologií, bude muset přijmout některé výše zmíněná opatření.

Zejména opatření na podporu kvalifikovaných lidských zdrojů, které budou pro stát pracovat na zabezpečování úkolů v kyberprostoru. Autor této práce tak podporuje i na své pracovní úrovni na Úřadu vlády ČR činnost nového Výboru pro digitální ekonomiku a společnost Rady vlády pro informační společnost, který jako hlavní poslání věnuje zvýšené prostředky na podporu úrovně digitálního vzdělávání v České republice, což významně rovněž zvýší efektivitu a možnosti obrany České republiky jako celku v kybernetickém prostoru.[147]

[147] Statut Rady vlády pro informační společnost, znění účinné od 1. září 2022. Čl. 7 odst. 1 písm. c).

Seznam zkratek

BIS	Bezpečnostní informační služba
BRS	Bezpečnostní rada státu
CERT	Anglická zkratka *"computer emergency response team"*. S touto zkratkou pracuji i některé zákony ČR, například zákon o kybernetické bezpečnosti. Právní řád ČR počítá s tzv. národním CERT a vládním CERT.
CIA	anglicky Central Intelligence Agency (tzv. Ústřední zpravodajská služba, hlavní rozvědka USA)
CMS nebo KIVS	Centrální místo Služeb a Komunikační infrastruktura Informačních systémů veřejné správy
CSIRT.CZ	CSIRT.CZ je Národní CSIRT České republiky (plnící úkoly národního CERT). Je provozován sdružením CZ.NIC dle veřejnoprávní smlouvy a dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
CZ.NIC nebo CZ.NIC z.s.p.o.	Název zájmové sdružení právnických osob založené předními poskytovateli internetových služeb v roce 1998, které má v současné době přes sto členů. CZ.NIC je provozovatel Národního CSIRT České republiky, tedy národního CERT.
CZK	Oficiální měnová jednotka České republiky, Česká koruna.
ČR	Česká republika
DESI	Digital Economy and Social Index (Index digitální ekonomiky a informační společnosti) - srovnání členských zemí Evropské unie z hlediska rozvoje digitálních služeb a digitální přívětivosti.

DIA	Digitální a informační agentura
americká DIA	Defense Intelligence Agency, americká obranná zpravodajská služba
DDoS	Útoky *"Distributed denial of service"*: paralyzování nebo znefunkčnění internetové služby nebo stránky s cílem znemožnit k ní přístup prostřednictvím přehlcení nebo přespamování požadavků zpravidla z několika počítačů naráz.
DNS	Anglická zkratka *"domain name system"* je v oblasti IT používána zkratka pro hierarchický a decentralizovaný systém doménových jmen.
ENISA	The European Union Agency for Cybersecurity, česky Agentura pro kybernetickou bezpečnost Evropské unie
EU/Unie	Evropská unie
FSB ФСБ	Federální služba bezpečnosti - kontrarozvědka Ruské federace Федеральная служба безопасности Российской Федерации
HDP nebo GDP	Hrubý domácí produkt z anglického GDP (Gross Domestic Product) - celková peněžní hodnota všech statků a služeb za dané období na určitém území.
IT a ICT	Informační technologie, popřípadě informační a komunikační technologie
MMR	Ministerstvo pro místní rozvoj
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NAKIT	Národní agentura pro komunikační a informační technologie, s.p.

NATO	Anglický zkratka *“North Atlantic Treaty Organization”*, Severoatlantická aliance
NATO CCDCOE	NATO Cooperative Cyber Defense Center of Excellence, česky Centrum koordinace kybernetické obrany NATO.
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrála pro kybernetickou bezpečnost
NCKO	Národní centrum kybernetických operací
NCSI	Nation cyber security index
NGA	National Geospatial-Intelligence Agency, americká zpravodajská služba
NSA	The National Security Agency (v překladu do češtiny Agentura národní bezpečnosti nebo také Národní bezpečnostní agentura) Vládní kryptologická zpravodajská služba USA, která je podřízena Ministerstvu obrany USA.
NRO	National Reconnaissance Office, americká zpravodajská služba zaměřená na satelitní obranu.
NÚKIB	Národní úřad pro kybernetickou bezpečnost
OECD	Organizací pro hospodářskou spolupráci a rozvoj
PRS	Public Regulated Service (veřejně regulovaná služba) v rámci projektu Galileo
PSP ČR	Poslanecká sněmovna Parlamentu České republiky
RF	Ruská federace

RIA	Estonský úřad pro informační systémy (estonsky *Riigi Infosüsteemide Amet*)
RVIS	Rada vlády pro informační společnost
SPCSS	Státní pokladna Centrum sdílených služeb, s.p.
SSSR USSR CCCP	Svaz sovětských socialistických republik, Union of Soviet Socialist Republics (Soviet Union) Союз Советских Социалистических Республик
SZR	Správa základních registrů
TLS a SSL	Protokol Transport Layer Security (TLS) a jeho předchůdce Secure Sockets Layer (SSL) jsou kryptografické protokoly poskytující možnost zabezpečené komunikace na Internetu pro služby jako www, elektronická pošta, internetový fax a další datové přenosy.
USA	United states of America (Spojené státy americké)
ÚSÚ nebo ÚOSS	Ústřední správní úřad neboli terminologií kompetenčního zákona ústřední orgán státní správy
ÚV ČR	Úřad vlády České republiky
ÚZSI	Úřad pro zahraniční styky a informace
VeKySIO	Velitelství kybernetických sil a informačních operací (organizačně pod armádou ČR)
VZ	Vojenské zpravodajství
ZS	Zpravodajské služby

Seznam použité literatury

Monografie

- DRMOLA, Jakub. Konceptualizace kyberterorismu. Vojenské rozhledy. 2013, č. 2.
- GIBSON William, Neuromancer, Laser-books, 2010, ISBN 978-80-7193-318-2.
- SKŘEJPEK Michal, KINCL Jaromír, URFUS Valentin. Římské právo, vydání 1.. Nakladatelství C. H. Beck. Datum vydání 1995. počet stran 408. ISBN: 80-7179-031-1.
- COLARIK, Andrew M. a Lech JANCZEWSKI. Managerial Guide for Handling Cyber-terrorism and Information Warfare.
- DENNING, Dorothy E. Activism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In iwar.org.uk [online]. [cit. 2023-03-10]. Dostupné z: http://www.iwar.org.uk/cyberterror/resources/denning.htm Archivováno.

Konferenční příspěvky

- Konference Den bezpečnější internetu 2023. In youtube.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://www.youtube.com/watch?v=DawSAQSLBrc

Právní předpisy a interní předpisy

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky,
- Listina základních práv a svobod, publikována v České republice jako Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení listiny základních práv a svobod jako součásti ústavního pořádku České republiky ,
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky,
- Směrnice Evropského parlamentu a Rady Evropské unie č. 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, tzv. Směrnice NIS,
- Washingtonská smlouva ze 4. dubna 1949,
- Zákon č. 12/2020 Sb., o právu na digitální služby, tzv. digitální ústava,

- Zákon č. 289/2005 Sb., o Vojenském zpravodajství,
- Zákon č. 150/2021 Sb.., pro obranu v kyberprostoru klíčová novela zákona o Vojenském zpravodajství,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, známý jako zákon o kybernetické bezpečnosti,
- Zákon č. 153/1994 Sb., o zpravodajských službách České republiky,
- Zákon č. 154/1994 Sb., o Bezpečnostní informační službě,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti,
- Zákon č. 240/2000 Sb., o krizovém řízení, známý jako krizový zákon,
- Zákon č. 2/1969 Sb., kompetenční zákon,
- Zákon č. 222/1999 Sb., o zajišťování obrany České republiky,
- Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů,
- Zákon č. 40/2009 Sb., trestní zákoník,
- Zákon č. 90/1995 Sb., jednací řád Poslanecké sněmovny,
- zákon č. 111/2009 Sb., o základních registrech,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Zákon č. 89/1995 Sb., o státní statistické službě,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 250/2017 Sb., o elektronické identifikaci,
- Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací,
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která má za cíl určit významné informační systémy veřejné správy a určení jejich kritérií,

- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,
- Vyhláška č. 315/2021 Sb., o bezpečnostních pravidlech cloud computingu
- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Interní předpisy a koncepční dokumenty:

- Usnesení vlády ze dne 18. ledna 2023 č. 48,
- Usnesení vlády ze dne 11. ledna 2023 č. 23,
- Usnesení vlády ze dne 12. dubna 2022 č. 15,
- Usnesení vlády ze dne 6. dubna 2022 č. 274,
- Usnesení vlády ze dne 21. prosince 2022 č. 1078,
- Usnesení vlády ze dne 21. 12. 2022 č. 1103,.
- Statut Bezpečnostní rady státu,
- Statut Rady vlády pro informační společnost,
- Důvodová zpráva k zákonu č. 289/2005 Sb., o Vojenském zpravodajství,
- Důvodová zpráva k zákonu č. 150/2021 Sb., kterým se mění zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a další související zákony,
- Národní strategie kybernetické bezpečnosti 2015-2020,
- Obranná strategie České republiky z roku 2017, Bezpečnostní strategie České republiky z roku 2015.

Webové stránky a elektronické zdroje

- Vzrůstající kriminalita v kyberprostoru. In mvcr.cz, 2020. [online]. [cit. 2022-11-05]. Dostupné z: https://www.mvcr.cz/clanek/pozor-na-kyberprostor-ministerstvo-vnitra-podporilo-prevenci-proti-kyberkriminalite-ve-videospotech-i-v-brozure.aspx
- Politics in the Digital Age. In academia.edu. [online]. [cit. 2023-11-29]. Dostupné z: https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age

- Terminologický slovník Ministerstva vnitra ČR. [online]. [cit. 2023-02-05]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx
- Prevence kriminality. In prevencekriminality.cz [online]. [cit. 2023-01-30]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/
- Hodnocení všech států světa v kybernetické bezpečnosti. In ncsi.ega.ee [online]. [cit. 2023-03-11]. Dostupné z: https://ncsi.ega.ee/ncsi-index/?order=rank
- Podvody s kryptoměnami. In finex.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://finex.cz/nejcastejsi-podvody-s-bitcoinem-na-toto-si-dejte-pozor/
- Legislativa kybernetické bezpečnosti. In nukib.cz. [online]. [cit. 2023-02-07]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
- What is Metaverse? In wired.com [online]. [cit. 2023-02-15]. Dostupné z: https://www.wired.com/story/what-is-the-metaverse/
- Mezinárodní kontakty BIS. In bis.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.bis.cz/mezinarodni-spoluprace/
- NATO, list of countries which agreed with Finland and Sweden accession to NATO. In nato-pa.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato-pa.int/content/finland-sweden-accession
- NATO Bucharest Summit Declaration. In nato.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato.int/cps/en/natolive/official_texts_8443.htm
- Spolupráce zpravodajských služeb. In bis.cz [online]. [cit. 2023-02-16]. Dostupné z: https://www.bis.cz/mezinarodni-spoluprace/mezinarodni-spoluprace-e769e1ea.html
- Výroční zpráva BIS. In bis.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/
- Programové prohlášení a poradce pro národní bezpečnost. In ceskenoviny.cz [online]. [cit. 2023-01-16]. Dostupné z: https://www.vlada.cz/programove-prohlaseni-vlady-193547

- Superúředník pro národní bezpečnost, krizový manažer a poradce v jednom. In natoaktual.cz. [online]. [cit. 2023-01-20]. Dostupné z: https://www.natoaktual.cz/zpravy/poradce-bezpecnost-obrana-vnitro-armada-namestek-koordinator.A210722_144606_na_zpravy_m00
- Nouzový stav při epidemii Covid-19. In covid.gov.cz. [online]. [cit. 2022-01-20]. Dostupné z: https://covid.gov.cz/situace/onemocneni-obecne-o-opatrenich/nouzovy-stav
- Informace Úřadu vlády o vládních usnesení ohledně boje s epidemií. In vlada.cz. [online]. [cit. 2022-03-10]. Dostupné z: https://www.vlada.cz/cz/epidemie-koronaviru/dulezite-informace/vladni-usneseni-souvisejici-s-bojem-proti-epidemii---rok-2021-193536/
- Vedení NÚKIB. In nukib.cz [online]. [cit. 2023-02-09]. Dostupné z: https://nukib.cz/cs/o-nukib/vedeni-uradu/
- Digitální a informační agentura. In profant.eu [online]. [cit. 2023-03-05]. Dostupné z: https://www.profant.eu/2022/dia.html
- Vize ředitele DIA. In lupa.cz [online]. [cit. 2023-02-26]. Dostupné z: https://www.lupa.cz/clanky/martin-mesrsmid-dia-chci-zaridit-abychom-nemuseli-s-urady-komunikovat-papirove/
- Estonský úřad pro informační systémy. In ria.ee [online]. [cit. 2023-01-16]. Dostupné z: https://www.ria.ee/
- Organizační schéma Úřadu vlády ČR. In vlada.cz [online]. [cit. 2023-01-16]. Dostupné z: https://www.vlada.cz/cz/urad-vlady/organizacni-struktura/organizacni-schema-uradu-vlady-cr-65949/
- Statut Rady vlády pro informační společnost, aktuální znění účinné od 1. 9. 2022. In mvcr.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.mvcr.cz/clanek/rada-vlady-pro-informacni-spolecnost.aspx
- Návrh nového systému financování strategických projektů. In army.cz [online]. [cit. 2023-01-07]. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/ministerstvo-obrany-predstavilo-navrh-noveho-systemu-financovani-strategickych-projektu-239124/
- Poptávka po IT odbornících. In novinky.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-v-cesku-chybi-okolo-20-000-it-specialistu-o-40-procent-vic-nez-loni-40407364

- Plat IT odborníka. In platy.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.platy.cz/platy/informacni-technologie
- Odměňování IT specialistů. In diit.cz [online]. [cit. 2023-02-11]. Dostupné z: https://diit.cz/clanek/jaky-je-prumerny-plat-v-it-staci-na-zivot-v-luxusu
- IT něco stojí. In lupa.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.lupa.cz/clanky/ivan-bartos-statnim-ajtakum-musime-zvysit-platy-na-sto-tisic-znalosti-neco-stoji/?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu
- Nejméně žen pracuje v českých firmách z celé EU. In mesec.cz [online]. [cit. 2023-02-11]. Dostupné z: https://www.mesec.cz/clanky/v-ceskych-firmach-pracuje-nejmene-zen-v-it-v-evrope-horsi-je-jen-madarsko/
- Proč právě Vojenské zpravodajství? In vzcr.cz [online]. [cit. 2023-03-04]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46
- Doporučení pro české olympioniky i veřejnost. In nukib.cz [online]. [cit. 2023-02-27]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1792-nukib-vydal-spolu-s-vojenskym-zpravodajstvim-doporuceni-pro-ceske-olympioniky-i-verejnost/
- Summit NATO ve Varšavě. In natoaktual.cz [online]. [cit. 2023-03-04]. Dostupné z: https://www.natoaktual.cz/projekty/special-summit-nato-ve-varsave-2016.A160405_144542_na_zpravy_m02
- Národní centrum kybernetických operacích. In ncko.cz [online]. [cit. 2023-03-04]. Dostupné z: https://www.ncko.cz/
- Schválení programu schůze za 30 hodin. In iprima.cz [online]. [cit. 2023-03-04]. Dostupné z: https://cnn.iprima.cz/snemovna-po-30-hodinach-schvalila-program-schuze-k-nizsimu-rustu-penzi-201789
- Two plus four agreement. In treaties.un.org [online]. [cit. 2023-02-18]. Dostupné z: https://treaties.un.org/doc/Publication/UNTS/Volume%201696/volume-1696-I-29226-English.pdf
- Dohoda 2+4. ct24.ceskatelevize.cz [online]. [cit. 2023-02-18]. Dostupné z: https://ct24.ceskatelevize.cz/archiv/1443337-znovusjednoceni-nemecka-historicky-podpis-smlouvy-2-4

- Promise to Gorbachev. In nsarchive.gwu.edu [online]. [cit. 2023-02-18]. Dostupné z: https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early
- Rusko rozšířilo seznam nikoliv přátelských zemí. In forbes.cz [online]. [cit. 2023-02-18]. Dostupné z: https://forbes.cz/rusko-rozsirilo-seznam-nikoliv-pratelskych-zemi-sve-financni-zavazky-jim-bude-splacet-jen-v-rublech/
- Aktuální seznam nikoliv přátelských zemí dle ruských zdrojů. In ria.ru [online]. [cit. 2023-02-18]. Dostupné z: https://ria.ru/20220722/nedruzhestvennye_strany-1804332755.html?in=t
- NATO Centrum pro kybernetickou obranu. In ccdcoe.ru [online]. [cit. 2023-03-04]. Dostupné z: https://ccdcoe.org/
- ENISA. In enisa.europa.eu [online]. [cit. 2023-03-04]. Dostupné z: https://www.enisa.europa.eu/
- Cyber Coalition 2022. In nato.int [online]. [cit. 2023-02-11]. Dostupné z: https://www.act.nato.int/cyber-coalition
- Kybernetická obrana České republiky. In vzcr.cz [online]. [cit. 2023-02-12]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46
- Cvičení NATO ohledně obranyschopnosti aliance v kybernetickém prostoru. In nukib.cz [online]. [cit. 2023-02-12]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1917-experti-nato-na-kybernetickou-bezpecnost-v-estonsku-pracovali-na-spolupraci/
- Estonsko v DESI indexu. In europa.eu [online]. [cit. 2023-02-12]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-estonia
- Mezinárodní telekomunikační unie. In itu.int [online]. [cit. 2023-02-12]. Dostupné z: https://www.itu.int/en/Pages/default.aspx
- Zneužívání falešného webu Portálu občana. In antivirovecentrum.cz [online]. [cit. 2023-03-11]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/podvodnici-zneuzivaji-falesny-portal-obcana.aspx
- Estonia 3. world best in cybersec. In e-estonia.com [online]. [cit. 2023-02-12]. Dostupné z: https://e-estonia.com/estonia-outranks-most-of-the-world-in-global-cybersecurity-index/

- Global Cybersecurity Index. In itu.int [online]. [cit. 2023-02-12]. Dostupné z: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- Strategie kybernetické bezpečnosti USA z roku 2018. In unt.edu. [online]. [cit. 2023-02-14]. Dostupné z: https://digital.library.unt.edu/ark:/67531/metadc1259394/
- Národní centrum kybernetické bezpečnosti USA. In cyber-center.org [online]. [cit. 2023-02-14]. Dostupné z: https://cyber-center.org/
- National Institute of Standards and Technology. In nist.gov [online]. [cit. 2023-02-14]. Dostupné z: https://www.nist.gov/
- U.S. Intelligence Community. In intelligence.gov [online]. [cit. 2023-03-01]. Dostupné z: https://www.intelligence.gov/
- Defense Intelligence Agency. In dia.mil [online]. [cit. 2023-03-03]. Dostupné z: https://www.dia.mil/
- Intelligence of USA. In informationweek.com. [online]. [cit. 2023-03-03]. Dostupné z: https://www.informationweek.com/leadership/intelligence-agencies-must-operate-more-like-an-enterprise
- SolarWinds explained. In techtarget.com. [online]. [cit. 2023-02-14]. Dostupné z: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
- Hacker attack 2016. In edition.cnn.com [online]. [cit. 2023-02-16]. Dostupné z: https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html
- Federal Security Service. In government.ru [online]. [cit. 2023-02-14]. Dostupné z: http://government.ru/en/department/113/
- Russia behind cyber attack on Czech institutions. In radio.cz [online]. [cit. 2023-02-16]. Dostupné z: https://english.radio.cz/interior-minister-russia-behind-cyber-attack-czech-institutions-8748268
- NATO's Open Doors Policy. In nato.int [online]. [cit. 2023-02-18]. Dostupné z: https://www.nato.int/docu/comm/1999/9904-wsh/pres-eng/04open.pdf

- The most powerful military in the world. In egscholars.com [online]. [cit. 2023-02-18]. Dostupné z: https://egscholars.com/2023/01/30/10-most-powerful-military-in-the-world-2022/
- Nostalgia for the USSR (průzkum v ruštině). In levada.ru [online]. [cit. 2023-02-26]. Dostupné z: https://www.levada.ru/en/2017/12/25/nostalgia-for-the-ussr/
- Soviet nostalgia. In washingtonpost.com [online]. [cit. 2023-02-26]. Dostupné z: https://www.washingtonpost.com/news/worldviews/wp/2014/06/09/calls-for-a-return-to-stalingrad-name-test-the-limits-of-putins-soviet-nostalgia/
- 75 % občanů Ruské federace si myslím, že doba SSSR byla nejlepší v historii Ruska. In themoscowtimes.com. [online]. [cit. 2023-02-26]. Dostupné z: https://www.themoscowtimes.com/2020/03/24/75-of-russians-say-soviet-era-was-greatest-time-in-countrys-history-poll-a69735
- Čína je vnímána jako hrozba pro NATO. In ceskatelevize.cz [online]. [cit. 2023-02-16]. Dostupné z: https://ct24.ceskatelevize.cz/svet/2994746-summit-nato-poprve-jako-moznou-hrozbu-vyslovne-zmini-cinu
- Čína protestovala proti sestřelení balonu. In cnn.com [online]. [cit. 2023-02-26]. Dostupné z: https://edition.cnn.com/2023/02/04/asia/beijing-reacts-us-jets-shoot-chinese-spy-balloon-intl-hnk/index.html
- Nový zákon o kybernetické bezpečnosti možnost připomínkovat. In osveta.nukib.cz [online]. [cit. 2023-02-18]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145&fbclid=IwAR2Ft8zvQa-KJ1NiBePvFCc3PSxvcIV6EmRCqk29Ot1uZ4h7KrGc69Bh1Aw
- Výbory Bezpečnostní rady státu. In mvcr.cz [online]. [cit. 2023-02-22]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-rada-statu-brs.aspx
- Phishing útoky na MPSV. In mpsv.cz [online]. [cit. 2023-02-18]. Dostupné z: https://www.mpsv.cz/-/falesne-domeny-napodobuji-web-mpsv-jde-o-phishing-stranky-jsou-jiz-zablokovany
- Informační systémy ve veřejné správy. In homel.vsb.cz, 2011. [online]. [cit. 2022-11-14]. Dostupné z: https://homel.vsb.cz/~dan11/is_skripta/IS%202011%20-%20IS%20ve%20statni%20sprave.pdf

- Doménová revoluce. In lupa.cz, 2002. [online]. [cit. 2022-11-14]. Dostupné z: https://www.lupa.cz/clanky/domenova-revoluce-ve-verejne-sprave/
- Digitální transformace, kapitola 1.2 v Národním plánu obnovy. In planobnovy.cz, 2023. [online]. [cit. 2023-02-26]. Dostupné z: https://www.planobnovycr.cz/digitalni-transformace-3
- Závažné nedostatky čerpání z evropských grantů. In ekonomickydenik.cz, 2023. [online]. [cit. 2023-02-26]. Dostupné z: https://ekonomickydenik.cz/ceska-republika-muze-prijit-o-miliardy-z-evropskych-grantu-inventura-mpo-zjistila-zavazne-nedostatky/