POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

BAKALÁŘSKÁ PRÁCE

2022 **MONIKA HAUSNEROVÁ**

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra bezpečnostních studií

Hybridní hrozby a státní bezpečnostní agenda v komparaci České republiky a Pobaltských států

Bakalářská práce

Hybrid Threats and State Security Agenda in the Comparision of the Czech Republic and Baltic States

Bachelor thesis

VEDOUCÍ PRÁCE:

Mgr. Štěpán STRNAD, PhD.

AUTOR PRÁCE:

Monika HAUSNEROVÁ

PŘEROV

2022

Čestné prohlášení

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

V Přerově dne ……

……

Monika Hausnerová

ANOTACE

Práce se zabývá popisem hybridních taktik a hrozeb, stejně jako obranou vůči nim. Především je zaměřena na Českou republiku a Baltské státy, tedy Estonsko, Lotyšsko a Litvu. Pozornost je věnována rozboru činností bezpečnostních institucí v každém státu a jejich kooperaci, včetně spolupráce s mezinárodními organizacemi. Další oblastí je zkoumání bezpečnostních rizik a vytvořených strategií, které by měly být uplatněny proti hybridnímu působení. Dle zjištěných informací je v závěrečné části práce proveden rozbor a implementace jednotlivých kroků, které by měly být podniknuty v boji proti hybridním hrozbám. Některé aspekty z bezpečnostní oblasti České republiky musí být do budoucna více rozpracovány a musí být vytvořeny nové plány při řešení nových krizí a rizik.

KLÍČOVÁ SLOVA:

Hybridní hrozby * dezinformace * propaganda * obrana * bezpečnostní strategie * Česká republika * Pobaltí * NATO * Rusko

ANNOTATION

Topic of this thesis is aimed on description of hybrid tactics and threats as well as defence against these threats. Its main subjects are especially Czech Republic and Baltic States, which means Estonia, Latvia and Lithuania. Part of the thesis is focused on the activities of security institutions of each state and their cooperation in the state and in the international organisations. Further area researches the security risks and strategies against hybrid threats. Based on discovered facts, there is analyse and implementation of single steps in the final part of the thesis. These steps should be held in combating hybrid threats. The Czech Republic has to focus on some areas of the security and develop it. Also, there must be new strategies for the new crises and risks created.

KEY WORDS:

Hybrid threats * disinformation * propaganda * defence * security strategy * Czech Republic * Baltics states * NATO * Russia

Obsah

Úvod

Lidstvo ve světě 21. století denně čelí mnoha výzvám. Díky globalizaci a propojení zemí se běžná bezpečnostní rizika jednotlivých států stávají nebezpečnými pro všechny státy světa. Za bezpečnostní hrozby, které nás ohrožují, můžeme nepochybně považovat všechny ekonomické a sociální krize, nemoci a epidemie (jako je ebola, AIDS nebo COVID-19). Celosvětová pandemie vytvořila prostor pro nové hrozby. Rozpoutala nesnášenlivost, novou vlnu dezinformací o nemoci, kybernetické útoky, mimo jiné na sledovací technologie. Způsobila pád ekonomiky, diplomatický, ale i politický tlak na přední politiky a představitele států. Nesmíme ale opomenout ani další krize, jako jsou mezinárodní i vnitrostátní konflikty, šíření zbraní hromadného ničení, včetně propojení teroristických organizací s organizovaným zločinem. K takovým hrozbám musíme postavit doprovodné jevy, a to přírodní a humanitární katastrofy. V těchto krizích se obtížně hledá jejich hlavní příčina, respektive viník. Existují ale i jiné formy hrozeb.

Novou formou jsou hybridní hrozby a válčení. Díky stále dostupnějším a výkonnějším technologiím se také zlepšují a inovují způsoby vedení konfliktů. Využití konvenčních vojenských metod se snížilo na minimum. Při hybridní kampani se využívají především nekonvenční metody. Jsou to informace získané zpravodajskými službami a jejich kontrarozvědnou činností, špionáž (včetně kybernetické špionáže), kybernetické útoky a šíření dezinformací. Taktiky vedení hybridní války se různí a neexistuje univerzální strategie k jejímu čelení. Cílem je podlomení důvěry občanů v demokratické zřízení, státní aparát, mezinárodní společenství či důvěru v renomované instituce. Středem pozornosti se při vedení hybridní kampaně stávají taky digitální technologie a kybernetický prostor. Útoky se zvyšují a stupňují, často zasahují více subjektů naráz. Je proto nutné zajistit dostatečnou a kvalitní obranu. Nové hybridní hrozby se týkají i České republiky, která jim čelí zejména v oblastech narušení ideových hodnot a ústavního uspořádání. Zájem na ovlivnění bezpečnostní situace v ČR mají především Rusko a Čína. K posilování svého vlivu využívají propagandu, dezinformace nebo politický nátlak. Podobná situace nastala i v Pobaltí, jenž se ocitá pod stálým nátlakem Ruské federace. Do budoucna je nutné vytvořit a implementovat strategické plány pro tento hybridní boj. Státy musí spolupracovat v rámci

mezinárodních společenství, zejména v rámci NATO, EU nebo menších regionálních uskupení jako je Visegradská skupina nebo Baltic Assembly.

Cílem této bakalářské práce je vyhodnocení a komparace bezpečnostní agendy Baltských států a České republiky. Práce je rozdělena do sedmi kapitol. První se věnuje samotným hybridním hrozbám, historii, principům a znakům, taktice, nejčastějším terčům a základním prvkům ochrany. Druhá až šestá kapitola je zaměřena na jednotlivé státy, tedy Českou republiku, Estonsko, Lotyšsko a Litvu. Jsou zde popsány taktiky hybridního působení a nejčastější bezpečnostní hrozby, jimž tyto země čelí. Všechny státy mají své bezpečnostní instituce, které vytvářejí strategie a krizové plány proti těmto hrozbám, včetně spolupráce s mezinárodními společenstvími. Součástí této práce je i jejich rozbor. Sedmá kapitola je finálně zaměřena na komparaci hybridních hrozeb a působení v ČR a Pobaltí s cílem doporučit rozvoj některých klíčových bezpečnostních oblastí.

1 Hybridní hrozby

1.1 Historie a vývoj definice termínu hybridních hrozeb

Užití termínu hybridní hrozba, asymetrická či hybridní válka se poprvé použilo již v 90. letech minulého století v USA. Tehdy pojem *hybridní* představoval směs harmonizovaných, souběžně vedených konvenčních a speciálních operací během nestandartních konfliktů, jako je vedení guerillové války, terorismu či informační války. Propagátorem byl po řadu let Frank Hoffman, který tento pojem sumarizoval ve svém článku na počátku 21. století. Hybridní válka se v roce 2007 stala vojenským termínem. Toto úsloví nabídlo během válek na středním východu alternativní pojmenování konvenčního a protipovstaleckého boje. Hybridní válka není novodobý fenomén, její prvky můžeme spatřit i v Peloponéských válkách nebo v některých válkách ve starověkém Římě. Zde využívali právě hybridní taktiku banditů a kriminálníků trénovaní vojáci, kteří předstírali boje, přepadali konvoje u silnic a kradli obléhací stroje.

Za hybridně vedenou válku považuje Hoffman rusko-čečenskou válku (1994–1996), válku Srbska s Kosovem (1998–1999) či sovětskou intervenci Afghánistánu během 80. let 20. století[1]. Hybridní válkou probíhající ve 21. století je například anexe Krymu a probíhající válka na Donbase na Ukrajině. V tomto konfliktu využilo Putinovo Rusko obrovské množství nástrojů: diplomacii, využívání různých forem informací, uzavírání přátelských smluv, prodeje zbraní nebo vojenské operace v blízkosti ukrajinských hranic kvůli zajištění údajného bezpečí. Označení *hybridní* je záležitostí západního světa a Rusko jej jako agresor striktně odmítá.

Historicky se hybridní taktiky válčení dají rozdělit dle teorie, která se objevila v knize *The Sling and the Stone: On War in the 21st Century* vojenského teoretika Thomas X. Hammese. Autor je zde rozděluje do čtyř období, respektive generací. V první generaci hybridního válčení byly veškeré aktivity prováděné státem, který používal taktiku linie, kolony a boje, při nichž byla uplatněna technologická

[1] STOJAR, R. *Vývoj a proměna konceptu hybridní války*. Vojenské rozhledy. 2017. [cit. 2021-07-16]. ISSN 1210-3292, 2336-2995. 12 s. Dostupné z: https://vojenskerozhledy.cz/kategorie-clanku/ozbrojene-konflikty/vyvoj-a-promena-konceptu-hybridni-valky

vyspělost za použití pušek a kulometů během 18. a 19. století. Druhá generace je charakterizována taktikou lineární palby a pohybu se zaměřením na nepřímou palbu pomocí dělostřelectva. Tato taktika byla uplatněna od druhé poloviny 19. století do první světové války. Třetí období kladlo důraz na rychlost, manévry a útoky na zadní oblasti, nikoliv do týlu armád a využívalo podpory vojenských vzdušných sil. Tato strategie dominovala během 20. století. Od 90. let 20. století se využívá nových prostředků k dosažení cíle, jak předpověděl Hammes. Ve čtvrté generaci hybridní války užívají jak státní, tak i nestátní aktéři nekonvenční vojenské strategie. Uplatňují se prvky partizánské války a povstání. Výhody konvenčního boje jsou kompenzovány a vytlačeny nekonvenčními válečnými prostředky. V této čtvrté generaci hybridního válčení se užívá taktéž terorismu, informací k podlomení vlády v existujícím státu a k jeho delegitimaci a ke stimulaci vnitřního sociálního rozpadu. Díky nim je snadněji dosaženo žádoucího konečného vojenského anebo politického stavu[2].

1.2 Definice pojmu hybridní hrozby

Je důležité zdůraznit, že téměř cokoliv může být nazváno a považováno za hybridní hrozbu. Pragmatické používání natahuje pojem do krajnosti, a tím se stává méně srozumitelným. Koncept hybridního vedení války je neohraničený. Jeho definice by měla být jasně daná, musí by být poukázáno na to, co hybridní válka je a co není[3]. Výsledkem velkého množství popisů hybridního válčení (poukažme na narativy USA, Izraele a Velké Británie) je, že žádná z nich nemůže být univerzálně aplikována a není univerzálně relevantní pro potenciální hybridní situace[4].

Obecně je obtížné odlišit pojem hybridní hrozby (*hybrid threats*) od takzvaného komplexního přístupu porozumět hrozbám (*comprehensive approach*), který byl užíván Severoatlantickou aliancí. *Comprehensive approach* zdůrazňuje, že

---

[2] McCULLOH TIMOTHY B. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* Kansas. [online]. 2012. [cit. 2022-07-16]. 61 s. Dostupné z: https://www.hsdl.org/?view&did=758318.

[3] BAHENSKÝ, V. *PARADOX OF HYBRID WAR: On Causes and Implications of Pragmatism in the Debate.* Obrana a strategie. [online]. 2018. s. 89-100 [cit. 2021-07-16]. ISSN 12146463. 12 s. Dostupné z: doi:10.3849/1802-7199.18.2018.02.089-100

[4] McCULLOH TIMOTHY B. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* …

konflikt lze vyřešit za kooperace vojenských prostředků s civilními jednotkami. Je zaměřen na integraci politické bezpečnosti, rozvoj právního státu, dodržování lidských práv a svobod a humanitární rozměr zahraničních operací. Měl by spojovat krátkodobé reakce na krizi a stabilizaci s dlouhodobou pomocí a rekonstrukcí. Je důležité znát politické, historické, vojenské, sociální souvislosti a aspekty[5].

Nynější pojetí hybridních hrozeb odkazuje na akce, metody a způsoby konfliktu, jež jsou vedeny státními či nestátními aktéry. Ty jsou realizovány pomocí konvenčních i nekonvenčních prostředků koordinovaných v rámci různých forem informační války, finanční války, sabotáží a kyberútoků bez ohledu na případný střet s mezinárodním řádem[6]. Cílem je především podlomit, poškodit nebo ovlivnit bezpečnostní a jiná rozhodnutí na místní, regionální nebo státní úrovni. To se děje skrze využití slabin protivníka, destabilizaci a zkomplikování vyhledávání původců těchto dějů. Konflikty jsou často charakterizovány směsí netradičních taktik, decentralizovaným plánováním a akcemi, včetně používání jak jednoduchých, tak i sofistikovaných inovativních technologií[7]. Rychlost, intenzita, a především rozsah těchto praktik se s dokonalejšími technologiemi zvyšuje a hybridní hrozby se tak stávají více nebezpečnými. Zítřejší konflikty nebudou jednoduše zařazeny mezi konvenční nebo nekonvenční, jejich rozdíly se stírají a množství použitých prostředků se znásobuje.

Mezi klasické nástroje hybridních hrozeb pod zkratkou DIMEFIL patří:

D) diplomacie (diplomatic) – ovlivňování a nátlak skrze diskusi a činy politické reprezentace;

I) informace (information) – masmédia, sociální sítě, propaganda a šíření dezinformací;

[5] GEDAYOVÁ, M. *Srovnávací studie: Komplexní přístup Severoatlantické aliance a Evropské unie při řešení krizí.* Ochrana & Bezpečnost [online]. 2015. [cit. 2021-08-05]. ISSN 1805-5656. 63 s. Dostupné z: http://ochab.ezin.cz/O-a-B_2015_A/2015_A_09_gedayova.pdf . S 1,2

[6] HOFFMAN, F. G. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac. [online]. 2007 [cit. 2021-07-16]. 72 s. Dostupné z: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[7] Gen. CONWAY. *A Cooperative Strategy For Maritime Security.* Washington. [online]. 2007. [cit. 2021-08-05]. 20 s. Dostupné z: https://www.uscg.mil/Portals/0/Strategy/MaritimeStrategy.pdf

M) ozbrojené složky (military) – výhružky skrze demonstraci vojenské síly, bojové použití armády, infiltrace do napadeného státu a jeho využívání;

E) ekonomika (economic) – tlak (embargo, sankce, zastavení dodávek energie nebo surovin, uzavření hranic, apod.);

F) finance (financial) – destabilizace měny, trhu, bank, ovlivňování klíčových finančních institucí;

I) zpravodajství (intelligence) – aktivity zpravodajských služeb, špionáž, získávání politických a státních činitelů k rozvracení státu;

L) veřejný pořádek a právní stát (law enforcement – elements of national power) – využití protistátních rozvratných činností k útoku na hodnoty, právní aspekty, společenské uspořádání[8].

Dle Davida Kilcullena, experta na protipovstalecký boj, mohou být dále hybridní hrozby popsány jako „*působení jakéhokoliv protivníka, který současně využívá, přizpůsobuje tradiční bojové operace, asymetrickou taktiku povstaleckých jednotek, teroristické útoky a kriminální aktivity za využití nových technologií*[9]*“.* Boj a užití zbraní se již nevztahuje jen na aktivitu armád a vojenské sféry. Hybridní válka odkazuje na širší rozsah aktivit, než jen na nepřímé a asymetrické metody boje. Může být zcela jasná (otevřená), anebo skrytá. Útočníci se primárně snaží dosáhnout destabilizace bez užití vojenských prostředků a vyhnout se ozbrojené agresi. Je ovšem velmi pravděpodobné, že do hybridních útoků zapojí i tradiční vojenské prostředky. Nyní jsou již tradičním prvkem při vedení asymetrické války kybernetické útoky v kyberprostoru. Jejich cílem je ohrožení kritické infrastruktury, měkkých, ale i tvrdých cílů, a tím tak snadněji dosáhnou destabilizace států. Je třeba upozornit, že jednotlivé komponenty hybridní války nemusí být nutně nebezpečné, hrozba spočívá právě v kombinaci a alternativního využití hybridních metod. Hybridní válčení je komplexní a nenajdeme k němu jednotlivý vzorec k jeho rozpoznání.

[8] MV ČR. *Co jsou hybridní hrozby*. Centrum proti terorismu a hybridním hrozbám. Praha. [online]. 2021. [cit. 2021-10-04]. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

[9] STOJAR, R. Vývoj a proměna konceptu hybridní války. Vojenské rozhledy. 2017. [cit. 2021-07-16]. ISSN 1210-3292, 2336-2995. 12 s. Dostupné z: https://vojenskerozhledy.cz/kategorie-clanku/ozbrojene-konflikty/vyvoj-a-promena-konceptu-hybridni-valky

Major americké armády Timothy B. McCulloh sestavil ucelenou teorii hybridní války na šesti principech:

1. složení hybridních sil je unikátní vzhledem ke kontextu sil;
2. mají specifickou ideologii;
3. vždy čelí existenční hrozbě;
4. v hybridní válce je mezi soupeři disproporční rozdíl ve schopnostech;
5. hybridní síla obsahuje jak konvenční, tak i nekonvenční komponenty;
6. využívají obranných operací[10].

Mezi znaky hybridní války však můžeme zařadit i jiné podmínky. Dají se vysvětlit na případu Ukrajiny v roce 2014:

- Napadená země bývá dlouhodobě špatně vedena a nenaplňuje své základní funkce. Populace je polarizována na venkov a město, bohaté a chudé, nebo například na etnické menšiny a majoritu (Rusy, Ukrajince);
- Potenciální útočník má určitý zájem na ohrožené zemi a její populaci. Může využít měkké nástroje, jako je ovládnutí médií a manipulovat s veřejným míněním nejen skrze média (RT, Hlas Ruska, Sputnik, tisková agentura ITAR-TASS a agentura RIA Novosti), včetně sociálních sítí (proruských blogerů);
- Napadená země nemůže efektivně kontrolovat své hranice a nemá spojence, na které by se mohla spolehnout (neúspěšný pokus o připojení do NATO).
- Útočník má nějakou hodnotu v mezinárodním společenství (Rusko jako tehdejší člen G8 a dalších důležitých mezinárodních uskupení), má na něj vliv a může uplatnit jeho verzi událostí[11].

[10] McCULLOH,T. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the Hybrid Threat New?...*
[11] JAGELLO 2000. *Hybrid warfare: A new phenomenon in Europe's security environment. Updated and extended 2nd edition.* Praha: Jagello 2000 for NATO Information Centre in Prague, 2016. 29 s. ISBN 978-80-904850-5-1.

Hybridní válčení můžeme také shrnout do dalších sedmi principů:

1. Kompozice hybridních sil a jejich účinky jsou jedinečné v každém jednotlivém případě;
2. S nimi souvisí specifické ideologie, které tvoří jednotnou organizaci, jenž je tvořena sociální, kulturní a náboženskou identitou hybridních sil;
3. Hybridní síla vnímá existenční ohrožení skrze potenciálního útočníka. Díky tomuto domnělému strachu opouští tradiční vojenská dogmata, aby dosáhla dlouhodobého přežití;
4. Obsahují méně konvenčních vojenských prostředků;
5. Obsahují také elementy konvenčních i nekonvenčních prostředků, díky jejich kombinaci vzniká jejich největší výhoda;
6. Jsou defenzivním typem operací;
7. Hybridní organizace používají při uplatňování hybridní síly přitažlivé taktiky, jak ve fyzické, tak v kognitivní oblasti, aby neustále odbíjely síly protivníka a jeho vůli je používat[12].

1.3 Terče hybridního působení

Nejčastějšími terči jsou v hybridní válce nepřátelé daného útočníka. Především se může jednat o politické subjekty, jednotlivé státy nebo mezinárodní instituce, které nesdílí tytéž hodnoty a zájmy. Jsou to USA, NATO, EU, tradiční politické strany (zelení, sociální demokraté), stoupenci sankcí vůči Rusku (Velká Británie, Německo), veřejnoprávní média a novináři (u nás Česká televize, Český rozhlas), papež, miliardáři zakládající vzdělávací fondy (Soros, Bezos, Gates) nebo veškeré neziskové organizace (Mezinárodní červený kříž, Amnesty International).

Terčem jsou všichni vzdělaní lidé a profesoři, rovněž kritice čelí i samotné univerzity. Bývá zpochybňována existence globálního oteplování a klimatických změn či význam ekologie. Spolu s celosvětovou pandemií je zpochybňován samotná existence nemoci, popírá se účinnost očkování a lidmi jsou snadno šířeny konspirační teorie spjaté s nemocí COVID-19.

[12] McCULLOH,T. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the Hybrid Threat New?...*

1.4 Obrana proti hybridním hrozbám

Hybridním hrozbám lze čelit jen a pouze díky komplexnímu celospolečenskému přístupu. Ten by měl zahrnovat bezpečnostní složky a orgány veřejné správy, stejně jako komerční, mediální, vzdělávací a neziskové sektory. Za klíčovou obranu proti hybridním hrozbám můžeme považovat bezpečnostní politiku. Pojem odkazuje na politickou koncepci a množství opatření daného státu, jehož úkolem je zajistit jak vnitřní, tak i vnější bezpečnost[13]. Dle definice Ministerstva vnitra České republiky z roku 2015 můžeme bezpečnostní politiku považovat za: „*Společenskou činnost, jejíž základ tvoří souhrn základních státních zájmů a cílů, jakož i hlavních nástrojů k jejich dosažení, směřující k zabezpečení státní svrchovanosti a územní celistvosti státu a jeho demokratických základů, činnosti demokratických institucí, ekonomického a sociálního rozvoje státu, ochrany zdraví a života občanů, majetku, kulturních statků, životního prostředí a plnění mezinárodních bezpečnostních závazků“.* Bezpečnostní politika je dle této definice postavena na pěti základních komponentech:

- Zahraniční politika v oblasti bezpečnosti státu;
- Obranná politika;
- Politika v oblasti vnitřní bezpečnosti;
- Hospodářská politika v oblasti bezpečnosti státu;
- Politika veřejné informovanosti v oblasti bezpečnosti státu[14].

Tím, kdo se stává největším a nejčastějším aktérem bezpečnostní politiky, jsou národní státy, mezinárodní organizace (OSN), mezivládní organizace (NATO) a regionální uskupení, která zajišťují integraci a spolupráci (EU). Velmi důležitým článkem je stát a jeho instituce, jenž se bezpečnostními aspekty zabývají nejvíce, především zpravodajské služby, kybernetické úřady nebo armáda.

Dnešní svět je přehlcen informacemi. Díky rozšířenosti internetu po celém světě se zde denně vyskytne více než 2 miliony nových článků a informací. Na sociálních sítích je toto číslo ještě vyšší. Ne všechny informace se dají označit jako spolehlivé

[13] DANICS Š., STRNAD Š. . *Aspekty bezpečnosti*. PAČR. 2016. ISBN 978-80-7251-455-7. S.58
[14] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Bezpečnostní strategie České republiky*. Praha. [online]. 2015. [cit. 2021-08-07]. ISBN 978-80-7441-005-5. 24 s. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

a pravdivé, proto je nutné si informace převzaté z kyberprostoru verifikovat a ověřovat. Ve velkém množství informací je nutné naučit se orientovat a rozlišit ty pravdivé od hoaxů. Ve světě existuje mnoho nezávislých platforem, jenž se touto problematikou zabývají a spolehlivě vyhodnocují pravdivé informace. Mezi tyto patří mimo jiné česká společnost *Semantic Visions*, která díky svému software založenému na OSINT (***O**pen **S**ource **IN**telligence*, tedy zpravodajství z otevřených zdrojů) analyzuje 90 % světového zpravodajského obsahu. Provozuje systém včasného varování v nejpoužívanějších jazycích a chrání dopředu své uživatele před dezinformacemi, propagandou a jinými hrozbami[15]. Dalšími, veřejně dostupnými weby zabezpečující analýzu informací, jsou například poynter.org, eufactcheck.eu.

Dezinformační weby či skupiny na sociálních sítích (Facebook, Twitter, YouTube atd.) užívají typická slovní spojení „*bez cenzury, nezávislý, nekorektní, svobodný, nenechme si diktovat, obyčejní lidé*“ apod. Cílem těchto zdůrazňujících přídavných jmen je dokazovat, že tyto informace jsou pravdivé, ale utajované. Tituly bývají pobuřující nebo morálně nekorektní, mohou obsahovat návodné otázky. Texty jsou doplněny o vulgarismy a opakováním jedné informace několikrát po sobě, aby se docílilo co největšího důrazu. Důsledkem je přitáhnutí chtěné pozornosti. Najdeme zde slovní spojení a útoky proti domnělým elitám, migrantům a jiným objektům. Videa na těchto platformách jsou opatřena titulky, vysvětlujícími probíhající dění na záběru vytrženém z kontextu. Divák je manipulován a je v něm záměrně vyvoláván strach. Z tohoto důvodu je nutné zabezpečit vzdělávání široké veřejnosti v oblasti mediální a internetové gramotnosti, a také zjistit, jak čelit novým nástrahám internetu. Naše společnost není schopna kriticky myslet, a proto by se do budoucna mělo dbát na rozvoj kritického myšlení již v raném dětském věku[16].

S tímto souvisí kybernetická ochrana před hybridními hrozbami. Technologický pokrok je nezastavitelný, vylepšování systémů se děje denně. Se zvyšujícím se počtem uživatelů digitálních technologií se navyšuje riziko zneužití personálních

[15] SEMANTIC VISIONS. *About us – Semantic Visions*. Praha: Semantic Visions. [online] 2021 [cit. 2021-10-04]. Dostupné z: https://semantic-visions.com/
[16] ALVAROVÁ A. Průmysl lži: propaganda, konspirace a dezinformační válka. 2., rozšířené vydání. Praha: Stanislav Juhaňák – Triton, 2019. 308 stran. ISBN 978-80-7553-682-2

informací, které tito uživatelé poskytují v kybernetickém prostoru. Je třeba vzdělávat a školit obyvatelstvo ohledně digitální hygieny, o tom, jak se bezpečně pohybovat na platformě jménem internet, jaká používat zabezpečení apod. Množství dat se přesunulo ze státních institucí do počítačových systémů, které se snadno stávají terčem kybernetických útoků.

2 Česká republika

Česká republika je v geopolitickém uspořádání světa pomyslným mostem mezi západem a východem Evropy. Se svými 78 866 km² je rozlohou srovnatelná se všemi třemi pobaltskými zeměmi dohromady, jimž bude v této bakalářské práci věnována pozornost. Politickým systémem je unitární parlamentní republika, stejně tak jako v Pobaltských státech.

V současné době má ČR po sčítání lidu 10,5 milionu obyvatel, jenž žijí na historických územích Česka, Moravy a Slezska. Národnostní menšiny tvoří 4,7 % obyvatel země, z nichž jejich nejvýraznější počet tvoří Slováci, Vietnamci a Ukrajinci. Na rozdíl od Pobaltí je obyvatelstvo ČR homogenní a nemá výrazné národnostní menšiny. Zároveň je svým počtem obyvatel poměrně větší.

Od 12. 3. 1999 je ČR členem NATO. Díky tomu získala záruku bezpečnosti proti potencionálním hrozbám. Dále byla přijata 1. 5. 2004 jako plnohodnotný člen Evropské unie. Tyto dvě členství v mezinárodních společenstvích jsou pro ČR klíčové, zejména díky záruce kooperace s ostatními státy Evropy, jak na poli ekonomickém, tak v oblasti bezpečnosti. Do budoucna jsou obě instituce zásadní pro vývoj ČR směrem vpřed.

2.1 Hybridní působení a bezpečnostní hrozby v České republice

Česká republika je vystavena hybridnímu působení sil zejména v oblastech, které jsou ideově a hodnotově zakotveny ve společnosti a v ústavním uspořádání státu. To se projevuje zejména v ovlivňování politických struktur a celkového rozhodovacího procesu, soudů, policie, ozbrojených sil, hromadných sdělovacích prostředků a veřejném mínění. Cílem veškerého hybridního snažení je narušení stability společnosti a vytvoření nedůvěřivého prostředí vůči občanům, a to včetně porušení ústavněprávního uspořádání státu.

Další oblastí ohrožení je **ekonomika**. Hybridní hrozby vůči ČR spočívají v zástavě dodávek strategických surovin ze zahraničí, jako je ropa nebo zemní plyn. Působení hybridního charakteru se může projevit i při využívání moderních technologií, například 5G sítí a umělé inteligence, které pocházejí ze zemí s odlišným ideologickým směrem. V rámci nových technologií se stupňuje riziko silnějších **kybernetických útoků**. Před nimi se snaží varovat, popřípadě dále řešit probíhající události Národní úřad pro kybernetickou a informační bezpečnost. Stále častější je napadání nemocnic a získávání citlivých informací. Tyto kyberútoky jsou provázány s kyberterorismem.

Ohrožení souvisí taktéž s korupcí, diplomacií, obchodem, špionáží nebo vystupování a hájení zájmů cizích států a mocností. Jedním ze zásadních problémů je **působení cizích států na našem území** v jejich prospěch, což může ohrozit bezpečnost v ČR. Jedná o dvě velmoci, Rusko a Čínu (zejména jejich zpravodajské služby), jenž jsou opakovaně zmiňovány v každoročních zprávách našich zpravodajských služeb. K posílení svého vlivu používají propagandu, šíření dezinformací a využívání komunikačních a informačních kanálů či nových technologií. Díky nim nepřímo ovlivňují veřejné mínění obyvatelstva, a vedou tak informační válku. Tradičně se tyto mocnosti také zaměřují na vybudování sféry vlivu prostřednictvím kombinace politického, vojenského a hospodářského nátlaku. Na našem území budují sítě vlivu mezi zástupci parlamentních politických stran, státními úředníky a lobbisty[17]. Ruské a čínské hrozby jsou podceňovány a bagatelizovány našimi zástupci na nejvyšších úrovních již řadu let. Svojí politikou vědomě nahrávají zájmům cizích mocností a oslabují naše vazby na EU a NATO.

Ruská vojenská rozvědka GRU měla pravděpodobně své centrum na ambasádě v Praze. Od roku 1996, kdy vychází výroční zprávy BIS, byla každoročně zaznamenávána aktivita ruských zpravodajských služeb v Česku. Jejich činnost byla oficiálně chráněna diplomatickou imunitou. V rámci Česko – Ruských vztahů došlo během roku 2021 ke vzájemnému vyhoštění diplomatů a administrativních

[17] MV ČR. *Audit národní bezpečnosti.* Praha. [online]. 2016. [cit. 2021-09-20]. 142 s. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf. s. 51.

pracovníků na ambasádách v Moskvě a v Praze. Česká republika vyhostila z ruské ambasády v Praze 18 diplomatů kvůli výbuchům muničního skladu ve Vrběticích v roce 2014. Výbuchy byly zapříčiněny právě ruskou vojenskou rozvědkou. Po odpovědi Ruska, tedy vyhoštění diplomatů z české ambasády v Moskvě, rozhodlo české ministerstvo zahraničí o snížení počtu ruských pracovníků na ambasádě v Praze. Jejich počet se snížil z 95 na 32. Díky tomu se dá do budoucna očekávat pokles cizí zpravodajské činnosti na území ČR.

Čtvrtým sektorem je **bezpečnost a ochrana.** Hybridní působení může mít za úkol zalarmovat a mobilizovat zájmové nebo kriminální skupiny k činnostem, jež vedou proti primárním bezpečnostním atributům České republiky, stejně jako k narušení veřejného pořádku[18]. Nebezpečný je politický extremismus, projevující se v silně polarizovaných názorech, které jsou zastíněny myšlenkou pravdivosti. Česká scéna pravicového i levicového extremismu je dlouhodobě monitorována bezpečnostními složkami a neuchyluje se k násilí. Napříč názorovými proudy se extremisté shodnou na jediném společném tématu, a to na nenávisti k určitým minoritním skupinám obyvatel. S postupující celosvětovou pandemií přešly na vlnu politického extremismu nové strany, činnost *Dělnické strany sociální spravedlnosti* nebo *Národní demokracie* ustoupila do pozadí. Nové extremistické spektrum tvoří především *Svoboda a přímá demokracie* (SPD)[19] nebo *Volný blok*. Tyto dvě strany rozšiřují hoaxy a dezinformace na sociálních sítích a na svých webových stránkách. Jejich členové pod nátlakem píšou či sdílejí články prospěšné pro stranu. Byli to právě oni, kdo se nejčastěji od března 2020 uchyloval ke kritice vládních opatřeních, bagatelizaci celé situace spojené s pandemií a přejímali různé konspirační teorie. Dlouhodobě požadují odchod ČR z NATO a EU (tzv. *Czexit*)[20]. Jejich politická vyhraněnost vážně ohrožuje demokratické základy ČR.

[18] MO ČR. *Národní strategie pro čelení hybridnímu působení.*[online] Praha. 2021. [cit. 2021-09-20]. 12 s. Dostupné z: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

[19] MV ČR. *Zpráva o extremismu a předsudečné nenávisti na území České republiky v roce 2020*. Ministerstvo vnitra, Odbor bezpečnostní politiky. [online] Praha. 2021. [cit. 2021-09-20]. 31 s. Dostupné z: https://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx

[20] SVOBODA A PŘÍMÁ DEMOKRACIE. *Volební program SPD*. [online]. 2021. [cit. 2021-08-09]. Dostupné z https://www.spd.cz/program-vypis/; VOLNÝ BLOK. *Volební program VOLNÉHO bloku*. [online]. 2021. [cit. 2021-08-09]. Dostupné z https://volnyblok.cz/ostatni/program-volneho-bloku/.

Bezpečnostní situace v Evropě je dlouhodobě zhoršená, zejména v důsledku pokračující migrační vlny od roku 2015, anexe poloostrova Krym, jakožto území suverénního státu nebo kvůli častým teroristickým útokům v Evropě. Hrozba terorismu jako metody násilného prosazování politických cílů je v České republice trvale poměrně nízká, ale možná. Charakteristickým rysem je existence nadnárodních sítí volně propojených skupin, které i bez jednotného velení sdílejí ideologii, cíle a plány k jejich naplnění, finanční zdroje či informace zvyšující ničivý potenciál jejich působení. Dle *Auditu národní bezpečnosti* z roku 2016 je pravděpodobnost výskytu teroristického činu útok na kritickou infrastrukturu ČR střední hrozbou. Některé prvky kritické infrastruktury je velmi obtížné střežit. Útoky na kritickou infrastrukturu jsou více nebezpečné, protože způsobují dalekosáhlejší škody, včetně těch sekundárních. Tato střední hrozba platí pro kritickou infrastrukturu, měkké cíle, zvlášť ohrožené objekty a osoby nebo české občany v zahraničí[21].

Za **velké slabiny,** které ohrožují vnitřní uspořádání státu, můžeme zmínit špatnou **odolnost obyvatelstva** a široké veřejnosti **proti** ovlivňování a **snahám snižovat důvěru v demokracii a právní systém státu**. To je zapříčiněno velmi nedostatečnou občanskou a mediální gramotností s kritickým myšlením, jimž se v naší společnosti věnuje málo prostoru. S tím souvisí neexistence nástrojů k obraně státu proti dezinformačním kampaním. Další slabou stránkou je působení politických subjektů, které neskrývaně obhajují zájmy, které se neztotožňují s primárními zájmy České republiky. Stejně tak jako působení a obhajoba bývalých i současných předních představitelů našeho státu odlišných zájmů, nebo zájmů třetích států s odlišnou politickou ideologií (jako je Rusko nebo Čína)[22]. K šíření dezinformací přispívají v české sféře sociální média a dezinformační weby a blogy. Nejznámějšími weby jsou *AC24, Sputnik CZ, Aeronet* nebo *Parlamentní listy*. Jejich návštěvnost se pohybuje okolo milionu měsíčně. Výjimkou jsou Parlamentní listy, jejichž návštěvnost je na 6 milionech (prosinec 2021[23]). Nejčtenější, částečně dezinformační web, dává prostor extremistickým

[21] MINISTERSTVO OBRANY ČR. *Audit národní bezpečnosti*…s. 27-38
[22] MINISTERSTVO OBRANY ČR. *Audit národní bezpečnosti*…s. 52
[23] SIMILAR WEB. *Parlamentní listy.* Similarweb.com. [online]. 2022. [cit. 2022-01-30]. Dostupné z: https://www.similarweb.com/website/parlamentnilisty.cz/#overview

vyjádřením a nezkoumá pravdivost zveřejněných tvrzení. Zprávy Parlamentních listů se překrývají se zprávami z webu Sputnik CZ, který je přebírá z ruských zdrojů[24]. V roce 2020 i 2021 tato média nadále produkovala xenofobní obsahy, dezinformace a konspirační teorie. Nejčastějšími tématy byly v roce 2021 nadále COVID-19, Rusko, Čína, Andrej Babiš a politika. Dezinformační média svou činností přispívali k polarizaci české společnosti a oslabování demokracie[25]. Příznivci xenofobních subjektů často opakují myšlenky produkované prokremelskou propagandou.

2.2 Bezpečnostní strategie ČR – instituce

Institucí, jenž je zodpovědná za čelení hybridnímu působení je primárně **vláda ČR**. Má stanoveny strategické cíle, jako je odolná společnost, stát i kritická infrastruktura, dále pak systémový a celostní přístup v rámci ČR a schopnost adekvátní a včasné reakce. V rámci vlády působí **Bezpečnostní rada státu**, která je jejím stálým orgánem v oblasti bezpečnostní problematiky. Primárním posláním je tvorba spolehlivého bezpečnostního systému státu, koordinace a kontrola takových opatřeních, jenž se vztahují k zajištění bezpečnosti ČR. Ve spolupráci s jednotlivými bezpečnostními radami krajů pravidelně vyhodnocuje potenciální rizika ohrožení státu a pravidelně předkládá vládě návrhy na nezbytná opatření ke snížení rizikovosti. Zároveň posuzuje momentální bezpečnostní situaci a možná rizika, opatření navrhovaná Ústředním krizovým štábem a koordinuje jeho činnost, pakliže by byl vyhlášen nouzový stav, stav ohrožení nebo válečný stav[26].

Bezpečnostní informační služba (BIS) je vnitřní zpravodajskou službou ČR. Její činnost nespadá pod žádný resort, je apolitická a nemá žádné represivní pravomoci. BIS uchovává důležité a tajné informace, ochraňuje demokracii, státní suverenitu a územní celistvost. Zároveň zjišťuje informace o zahraničních

[24] ČEŠTÍ ELFOVÉ. *Analýza: Překryv Parlamentních listů a ruského Sputniku.* [online]. 2021. [cit. 29.01.2022]. Dostupné z: https://cesti-elfove.cz/analyza-prekryv-parlamentnich-listu-a-ruskeho-sputniku/

[25] MVČR, odbor bezpečnostní politiky. *Zpráva o extremismu a předsudečné nenávisti na území České republiky v roce 2020…*

[26] VLÁDA ČR. *Statut Bezpečnostní rady státu*. Příloha č. 1 k usnesení vlády ze dne 9. července 2014 č. 544 ve znění usnesení vlády ze dne 10. května 2017 č. 360, usnesení vlády ze dne 18. dubna 2018 č. 247, usnesení vlády ze dne 10. července 2018 č. 457 a usnesení vlády ze dne 24. října 2018 č. 692 .[online]. 2018. [cit. 2021-10-04]. 5 s. Dostupné z https://www.vlada.cz/assets/ppov/brs/Statut-BRS-rijen-2018.pdf

zpravodajských službách, které operují v ČR, aktivitách jednotlivých subjektů, které by mohly zneužít utajované bezpečnostní informace nebo narušit ekonomickou stabilitu. Snaží se preventivně působit proti organizovanému zločinu a terorismu. Odkryté informace poskytuje prezidentovi, vládě, státním a policejním orgánům[27]. Svá zjištění zveřejňuje ve výročních zprávách. **Úřad pro zahraniční styky a informace** (ÚZSI), včasně zjišťuje a vyhodnocuje nebezpečí, která plynou ze zahraničních aktivit a narušují bezpečnost a zahraničně ekonomické zájmy ČR. Tyto informace nejsou běžně dostupné a pro jejich získání se musí použít nadstandartní prostředky a aktivity. ÚZSI je povinna tyto poznatky včasně vyhodnotit a předat ústavním činitelům a orgánům státní správy[28]. **Vojenské zpravodajství** je jednotnou ozbrojenou zpravodajskou službou ČR, zároveň je součástí Ministerstva obrany. Činnost zahrnuje vnitřní i vnější aktivity ZS a jejím cílem je sbírat a vyhodnocovat informace důležité pro obranu země pomocí zpravodajských větví HUMINT, SIGINT, IMINT i OSINT[29].

Resortem v rámci vlády zabývajícím se bezpečnostní otázkou, je **Ministerstvo vnitra ČR** (MVČR). Zajišťuje vnitřní pořádek a bezpečnost, analyzuje trendy vývoje, zabývá se tématy v oblasti cizinecké a pobytové politiky, udělováním občanství, atd. Pod jeho patronátem operuje **Policie ČR**, respektive Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování, jejíž významná role spočívá v řešení projevů cizí moci na úrovni trestného činu. Zároveň je kontaktována při šíření závadného obsahu a aktivit v kyberprostoru. Na základě Auditu národní bezpečnosti vzniklo v roce 2017 v rámci MVČR **Centrum proti terorismu a hybridním hrozbám**. Jeho cílem je osvěta, analýza vnitřní bezpečnosti, dezinformačních kampaní a jejich vyvracení.

Dalším řešitelem problematiky spjaté s hybridními silami a hrozbami na území ČR je **Národní bezpečnostní úřad** (NBÚ). Jeho cílem je zajišťovat obranu, kybernetickou bezpečnost v kritické infrastruktuře a IT, a zároveň chránit

[27] POKORNÝ L.; CHROBÁK J.; FLIEGEL M. *Zákon o zpravodajských službách České republiky. Zákon o Bezpečnostní informační službě. Zákon o vojenském zpravodajství. Komentář.* Praha: Wolters Kluwert. ČR. 2018. 204 s. ISBN 978-80-7552-378-5.
[28] ÚZSI. *Kdo jsme – ÚZSI.* Praha. [online]. 2021 [cit. 2022-10-04]. Dostupné z: www.uzsi.cz
[29] POKORNÝ L.; CHROBÁK J.; FLIEGEL M. *Zákon o zpravodajských službách České republiky. Zákon o Bezpečnostní informační službě. Zákon o vojenském zpravodajství. Komentář…*

utajované informace. Hlavním úkolem je vydávat osvědčení o bezpečnostní způsobilosti fyzickým i právnickým osobám. Díky této pravomoci je zajištěno, že utajované informace důležité pro obranu, armádu, bezpečnost, ekonomiku a mezinárodně politické cíle ČR zůstanou i nadále neveřejné i přes to, že jsou svěřené do rukou dalších subjektů[30]. **CSIRT.cz** je akreditovanou institucí poskytující řešení při incidentech ohrožující bezpečnost ČR pod záštitou NBÚ. Kooperuje se světovými CERT organizacemi (***C****omputer* ***E****mergency* ***R****esponse* ***T****eam)* a bezpečnostními složkami ČR, včetně státních úřadů. Poskytuje také vzdělávání v kybernetickém prostoru[31].

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je správním orgánem pro kybernetickou bezpečnost a zajišťuje ochranu utajovaných informací v IT a jiných komunikačních systémech. Mimo jiné připravuje národní bezpečnostní standardy v oblasti kyberbezpečnosti, včetně standardů pro informační systémy důležité pro kritickou informační infrastrukturu. NÚKIB je zásadním orgánem při přípravě zákonů a podzákonných norem v oblasti kybernetické bezpečnosti a jeho činnost se zaměřuje také na tvorbu národní strategie kyberbezpečnosti. Jeho nedílnou součástí je **Národní centrum kybernetické bezpečnosti**, které zajišťuje osvětu i prevenci před kyberhrozbami útočícími na kritickou informační infrastrukturu, informační systémy veřejné správy a klíčové instituce ČR. Další náplní je spolupráce s národními i mezinárodními organizacemi zaměřenými na bezpečnost v oblasti kyberprostoru, výzkum a vývoj[32].

Neopomenutelnou institucí, jenž se zajišťuje o celkovou bezpečnost České republiky, je **Armáda ČR** (AČR). V současné době má celkem 26 928 vojáků z povolání a dalších 3 615 v zálohách[33]. AČR představuje pojistku při čelení ozbrojeného konfliktu na území ČR, respektive při obraně některého ze členů NATO dle článku 5. V rámci NATO má armáda zastoupení v NATO Response

[30] NBÚ. *O nás – NBÚ*. Praha. [online]. 2021. [cit. 2022-10-04]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/#otazka01
[31] CSIRT.cz. *O týmu CSIRT.cz.* ČR. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://csirt.cz/cs/o-nas/
[32] NÚKIB. *NÚKIB.* Praha. [online]. 2021. [cit. 2021-10-04]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
[33] Počet aktualizovaný k 17. 1. 2022

Force, EU Battle Groups nebo v rámci posílené předsunuté vojenské přítomnosti na východě Aliance v Pobaltí (enhanced Forward Presence)[34]. Do obranného rozpočtu NATO přispívá ČR asi 1,05 % ročně. Armáda je plně připravena pohotově reagovat na krizové situace: podpořit civilní orgány zejména při živelních katastrofách, ke zvládání situace v nemocnicích (jak jsme se přesvědčili při pandemii COVID-19) nebo mohou být nápomocni při zásazích IZS.

2.3 Bezpečnostní strategie – základní dokumenty

2.3.1 Audit národní bezpečnosti 2016

Audit byl vypracován na pokyn Ministerstva obrany ČR s cílem analyzovat dosavadní bezpečnostní situaci a vytvořit plán, jak zajistit, aby se předcházelo potenciálnímu ohrožení státu. Dokument se zaměřuje na segmenty terorismu, extremismu, organizovaného zločinu, působení cizí moci na území ČR nebo na občany ČR v zahraničí, bezpečnostní aspekty migrace, přírodní a antropogenní hrozby, hrozby v kyberprostoru, energetickou, surovinovou a průmyslovou bezpečnost a také na hybridní hrozby a jejich vliv na bezpečnost občanů ČR.

S hybridními hrozbami nepřímo souvisí všechny výše jmenované segmenty. Obecně je nutné obrátit pozornost k problematice radikalizace a rekrutování obyvatelstva a průběžně náchylné a rizikové skupiny obyvatel monitorovat. Dále je důležité posílit ochranu fyzické i kybernetické kritické infrastruktury, navýšit personální kapacity pracovníků v oblasti krizového řízení a zajistit dostatečné financování při řešení mimořádných krizových událostí. Nejdůležitější je zajistit digitalizaci státní správy (s paralelním papírovým zálohováním), která učiní transparentnost a urychlí celý systém. S tím souvisí adekvátní a efektivní zabezpečení. V některých aspektech je třeba změnit a novelizovat legislativu (český Trestní zákoník má mezery v oblasti kybernetické trestné činnosti a trestnými činy spojenými se šířením dezinformací) a připravit a průběžně aktualizovat dlouhodobé strategie a vládní materiály. Je nutné zvýšit množství odborného, ale i administrativního personálu v bezpečnostní sféře a povinně jej spolu s obyvatelstvem vzdělávat, aby se zvýšila spoluodpovědnost občanů za

[34] ARMÁDA ČR. *Obranná strategie České republiky*. Praha. [online]. 2017. [cit. 2022-01-20]. 16 s. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/Obrann___strategie_2017_-_CZ.pdf. s.11-13

bezpečí. Do budoucna je třeba kooperovat se státními, nestátními a neziskovými organizacemi.

Kvůli ochraně státu před působením cizí moci je třeba dbát zvýšenou pozornost k **ovlivňování veřejného mínění** a **zisk zákonem chráněných informací** nebo jiných veřejně nepřístupných informací, jejichž znalost může vést k ohrožení či poškození zájmů státu. K posílení odolnosti Audit doporučuje, aby bylo implikováno efektivní školení všech článků společnosti – státních úředníků, jenž se mohou stát potenciálními prostředníky v poskytování citlivých a utajovaných informací pro cizí mocnosti (kvůli svému postavení se mohou stát zájmem cizí moci), ale i studentů škol skrze úpravu vzdělávacích plánů a díky posílení výuky občanské gramotnosti a zavedení výuky mediální gramotnosti[35].

Další oblastí, která představuje hybridní ohrožení ČR jsou **hrozby probíhající v kyberprostoru**, kybernetická špionáž, narušení nebo snížení odolnosti IT infrastruktury, nepřátelské kampaně nebo kyberterorismus. Prostor pro zlepšení nabízí Audit v podobě dostatečné alokace finančních prostředků v oblasti kyberbezpečnosti a její systémové řešení, bezpečnostní prověrka zaměstnanců a odborných pracovníků. Dále pak re-prioritizace resortů a institucí vzhledem k plánování investic do bezpečnostních technologií a informačních systémů a především, již zmíněná úprava legislativy.

Pravděpodobnost, že bude Česká republika vystavena hrozbě hybridního působení osamoceně, je téměř nulová. Úsilí, jak čelit hybridní kampani, je zformulováno NATO a EU ve *Strategii pro úlohu NATO v boji proti hybridnímu válčení* a v dokumentu *Společný rámec pro boj proti hybridním hrozbám: Reakce EU*. Jak už bylo mnohokrát zmíněno, zásadní pro bezpečnost ČR je součinnost s těmito dvěma nadnárodními mezinárodními organizacemi. ČR by se měla aktivně zapojovat do těchto strategií, pomoci při případném napadení a využít podpory, pakliže by se sama stala napadenou zemí[36].

[35] MV ČR. *Audit národní bezpečnosti*... s. 50-61
[36] MV ČR. *Audit národní bezpečnosti*... s.131.

2.3.2 Národní strategie kybernetické bezpečnosti České republiky

Kybernetická bezpečnost a její výhled byl vypracován NÚKIB na období let 2021 až 2025. Tato strategie vyzdvihuje jednotný přístup a vnímání kybernetické bezpečnosti a obrany nade všechno. Díky tomuto je možné vytvářet preventivní kroky pro zvládání krizových situací v kyberprostoru. Důležití jsou také jednotliví uživatelé kybernetického prostoru. Posilování internetové gramotnosti či kritického myšlení obyvatelstva jsou nezbytné kroky při čelení kybernetickým hrozbám stejně jako dostatečné finanční zdroje pro zabezpečení rozvoje, včetně vzdělávání odborníků. Také je třeba pokračovat v tvorbě funkčního modelu pro zajištění kybernetické obrany ČR. Je nutné, aby ČR vyhodnocovala kybernetické hrozby v širším kontextu, díky nim bude schopna jim efektivně a cíleně čelit. Nastavení bezpečnostních požadavků na zabezpečení soukromé i státní sféry by mělo být prioritou, včetně zálohování dat v cloudech[37].

Je třeba zajistit mezinárodní kooperaci s jednotlivými institucemi, které pomohou ČR jednotně a cíleně čelit hybridním hrozbám. Důležitá je také strategická komunikace a civilně-vojenská spolupráce. Prioritou je především posilovat naše postavení a hájit bezpečnostní zájmy ČR v rámci klíčových mezinárodních společností jako EU, NATO, OBSE, OECD a OSN[38].

2.3.3 Obranná strategie ČR a Dlouhodobý výhled pro obranu 2035

Obranná strategie ČR (2017) a Dlouhodobý výhled pro obranu jsou důležitými dokumenty Ministerstva obrany, které rozpracovávají přístup vlády ČR k zabezpečení země. Strategie se zaměřuje na současnou situaci ve světě a na současný stav obrany ČR. Popisuje její stav a systém. Pro Českou republiku jsou důležité 3 pilíře: zodpovědný přístup státu k obraně republiky a spojeneckým závazkům, akceschopné ozbrojené síly a občanská povinnost k obraně státu. Je nutné zajistit kvalitní obranu státu skrze účinné propojení jednotlivých složek,

[37] NÚKIB. *Národní strategie Kybernetické bezpečnosti České republiky.* In: Praha. [online]. 2020. [cit. 2021-10-13]. 24 s. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[38] MINISTERSTVO OBRANY ČR. *Národní strategie pro čelení hybridnímu působení.* Praha. [online] 2021. [cit. 2021-10-13]. Dostupné z: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

navýšení vojenského rozpočtu, nebo kapacit. Do budoucna je třeba podporovat členství v mezinárodních společenstvích a vytvářet a aktualizovat společné plány[39].

Dlouhodobý výhled pro obranu 2035 klade důraz na zajištění odolnosti společnosti, státu i kritické infrastruktury. Toho lze dosáhnout jen díky posílení schopnosti včasné detekce nepřátelských hybridních aktivit a adekvátní reakce na ně, využití transparentního systému prověřování zahraničních investic, které jsou důležité pro kritickou infrastrukturu státu (jako je například dostavba jaderné elektrárny v Dukovanech). Kritická infrastruktura bude podrobována zátěžovým testům simulujících hybridní působení, aby se zajistila její plnohodnotná funkce i v případě napadení. Také je důležité snížit závislost ČR na zemích, které se ideově a hodnotově liší (ČLR, Rusko). Pro naplnění těchto cílů je zásadní posilovat meziodborovou kooperaci a strategicky sdílet informace. Zároveň je třeba zajistit připravenost celého bezpečnostního systému skrze cvičení na národní a mezinárodní úrovni[40].

V rámci obrany je důležité usilovat o rozvoj v odvětví kybernetiky, především kybernetického prostoru a implementace nových průlomových technologií. Tím se rozumí robotizace, kybernetika a umělá inteligence. V rámci kyberprostoru je nutné do budoucna klást důraz na efektivní součinnost VZ a ozbrojených složek, a také na aktivní kybernetické působení při vedení komplexních bojových činností v kyberprostoru. Předpoklady pro naplnění těchto cílů jsou existence dostatečných zdrojů v obranném rozpočtu, stabilní prostředí pro personální rozvoj ozbrojených sil, propojený systém vyzbrojování a podpora obranného průmyslu (využívání výzkumu, vývoje a inovací). Roční podíl HDP v rozpočtu obrany v průměru z let 2014–2020 činí 1,26 % (k porovnání Estonsko vynakládá 2,38 %, Lotyšsko 1,75 % a Litva 1,73 %[41]). Kvůli novým technologiím je třeba, aby tento

[39] MINISTERSTVO OBRANY ČR. *Obranná strategie České republiky.* Praha. [online]. 2017. [cit. 2021-10-13]. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/Obrann___strategie_2017_-_CZ.pdf

[40] MO ČR. *Dlouhodobý výhled pro obranu 2035.* Praha. [online]. 2019. [cit. 2021-10-13]. Dostupné z: https://www.mocr.army.cz/images/id_40001_50000/46088/2035.pdf

[41] SIPRI. *Military expenditure by country as percentage of gross domestic product, 1988-2020.* SIPRI. [online]. 2021. [cit. 2021-10-13]. Dostupné z: https://sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%E2%80%932020%20as%20a%20share%20of%20GDP%20%28pdf%29.pdf

rozpočet byl navýšen a dosáhl patřičné hodnoty, díky které se vytyčené priority budou moci naplnit.

3 Pobaltské státy

Země Pobaltí, tedy Litva, Lotyšsko a Estonsko zaujímají svou polohou strategické místo na mapě světa. Jakožto sousední státy Ruska, a zároveň poslední státy NATO a EU ve východní Evropě, jsou „nárazníkem“ mezi východním a západním světem. Celkovou rozlohou zabírají 175 116 km², čímž jsou srovnatelné s rozlohou České republiky. Tyto státy jsou obklopeny velkými národy a potřebují dlouhodobou, neustálou ochranu, aby zůstaly suverénními.

V současné době má Pobaltí nízký počet obyvatel. Od rozpadu SSSR ztratily baltské státy ¼ celkové populace. To má nyní vliv na nízkou porodnost, vyšší procento sebevražd a vysoký podíl úmrtí. Mladí lidé migrují ve velkých počtech kvůli nepříznivé ekonomické situaci do zemí západní Evropy. Celková populace Litvy, Lotyšska a Estonska je tak stejná jako před rokem 1930. V Pobaltí k roku 2016 bylo přibližně 6,6 milionu obyvatel, z nichž v jednotlivých státech žije velké procento ruských menšin (v Litvě 5,8 %, Lotyšsku 24 % a Estonsku 23 %). Pro státy Estonska a Lotyšska, které mají nejvíce rusky mluvících obyvatel, je společná jejich nízká integrace s Estonci a Lotyši. Ruština není v žádné ze států oficiálním úředním jazykem. I přesto stále přetrvává rozdělení škol, kde se vyučuje jen rusky, anebo jen estonsky a lotyšsky. Mnoho obyvatel nemá žádné občanství (v Estonsku 77 300[42] a v Lotyšsku 209 000[43]), nemůže se účastnit voleb a celkového politického života.

Od 29. 3. 2004 jsou země členy NATO. Toto členství bylo jejich bezpečnostní prioritou kvůli vysokému stupni napětí ze strany Ruské federace, zejména v Kaliningradské oblasti, zesílenou po násilné anexi Krymu. Pobaltské státy vidí hrozbu ze strany Ruska v destabilizaci společnosti a radikalizaci početných ruských minorit. Od roku 2016 se v těchto třech státech pohybují stálé jednotky eFP NATO s cílem zajistit dohled nad bezpečnostní situací. Dále byly všechny státy přijaty 1. 5. 2004 jako plnohodnotní členové Evropské unie, a v roce 2015 se

[42] Republic of Estonia: Ministry of Interior. *Citizenship and Migration*. Estonia. [online]. 2020. [cit. 2021-11-15]. Dostupné z: https://www.siseministeerium.ee/en/activities/citizenship-and-migration#:~:text=As%20of%20January%202018%2C%2077%2C268%20persons%20with%20undetermined,590%20of%20them%20were%20persons%20with%20undetermined%20citizenship

[43] Republic of Latvia: Ministry of Interior. *Latvijas iedzīvotāju sadalījums pēc valstiskās piederības*. Latvia. [online]. 2020. [cit. 2021-11-15]. Dostupné z: https://www.pmlp.gov.lv/sites/pmlp/files/media_file/isvp_latvija_pec_vpd.pdf

země připojily k Eurozóně. Celkově jsou NATO i EU velmi důležité a zaručují se za bezpečnou a stabilní situaci v Pobaltí.

Díky tomu, že byly Baltské státy součástí SSSR je i dnes patrná vazba na Rusko. Všechny hlavní trasy dopravy, zemního plynu a elektřiny vedou právě odtud. K docílení plné nezávislosti je třeba posílit obchod v rámci EU a menších mezinárodních uskupení. Dále je nutné co nejdříve začít s výstavbou trasy *Rail Baltica*, která má vytvořit osu Varšava – Kaunas (Litva) – Riga – Tallinn – Helsinky. V neposlední řadě je třeba zajistit dodávky energií s Finskem, Švédskem a Polskem. Tím se zmenší závislost Estonska, Lotyšska i Litvy na Rusku.

Bezpečnostní situace v Evropě závisí na světové ekonomické stabilitě, bezpečném vývoji v kyberprostoru, zvyšování obraně proti technologickým a jiným hrozbám. Je proto důležité, aby státy ve spolupráci s mezinárodními společenstvími adekvátně reagovali na toto nebezpečí.

3.1 Společné instituce pro kooperaci Pobaltských států

Pro Pobaltí je nejdůležitější institucí zajišťující bezpečnost NATO a aktivní participace v jeho programech. Roku 2016 v rámci summitu ve Varšavě bylo odsouhlaseno, že v Pobaltí a Polsku budou rozmístěny mnohonárodnostní prapory NATO **enhanced Forward Presence** (eFP) o síle asi 4 500 vojáků[44]. V Estonsku sídlí ve městě Tapa, velitelským státem je Velká Británie (společně s Dánskem, Francií a Islandem), v Lotyšsku se sídlem v Adazi a velitelstvím Kanady (s vojáky ČR a dalších 8 států) a v Litvě Rukola (s vojáky ČR a 5 států NATO). Tyto prapory jsou plně schopny boje a představují ochranu východní hranice NATO a bezprostřední reakci na Ruskou agresi[45].

Dalším prvkem přispívajícím k ochraně Baltského moře je projekt zvaný **BALTRON**. Ochranu vzdušného prostoru podporuje **BALTNET**, tedy *Baltic Air Survelliance Network*. Tyto dvě společenství zaručují přímou protekci nad

[44] NATO. *NATO's Enhanced Forward Presence*. [online]. 2019. [cit. 2022-01-22]. Dostupné z: https://www.mfa.gov.lv/en/media/2228/download
[45] ALLIED LAND COMMAND NATO. *EFP*. [online]. 2022. [cit. 2022-01-22]. Dostupné z: https://lc.nato.int/operations/enhanced-forward-presence-efp

prostorem těchto zemí, spolupráci armád, podporují alokaci zdrojů tam, kde je potřeba a starají se o společný výcvik armád.

Společenstvím sdružujícím státy Pobaltí, Finska, Skandinávie, Islandu a Dánska je **Nordic-Baltic Cooperation** (NB8). Cílem je spolupráce, zahraničně politický dialog, otázka civilní bezpečnosti, kybernetické bezpečnosti, obranná spolupráce a energetiky. Diskuse je rozvíjena na každoročních summitech a NB8 navrhuje mimo jiné: pořádat národní cvičení a simulace nenadálých útoků, úzkou spolupráci s Cooperative Cyber Defence Centre of Excellence (CCDCOE) a vytvoření neformální severo-baltské kybernetické bezpečnostní sítě[46].

Baltic Assembly (BA) je regionálním sdružením mezi Estonskem, Lotyšskem a Litvou. Na posledním 40. zasedání během listopadu 2021 vyhodnotilo BA mezi největší priority sledovat současnou situaci v sousedních státech, zejména pak v Bělorusku, a vytvořit praktický plán pro zvýšení odolnosti proti hrozbám. Další prioritou bylo stanoveno vyčlenit prostředky CCDCOE pro rozšíření a posilování kybernetické obrany pomocí cílených cvičných útoků v regionu, včetně podpory přeshraniční kybernetické spolupráce. BA dbá na rozvoj digitalizace. Cílem je digitální technologická transformace EU (přeshraniční digitální služby, výměna dat a uznávání e-ID). Dalším jsou společné datové standardy a odstranění legislativních a administrativních překážek v rámci Pobaltí[47].

3.2 Hybridní působení a bezpečnostní hrozby v Pobaltí

Nejviditelnější hybridní aktivity na území Pobaltí vykazuje Ruská federace, která vede agresivní zahraniční a bezpečnostní politiku. Po válkách na Ukrajině a v Gruzii může Rusko projevit svůj mocenský zájem o Estonsko a Lotyšsko. V Estonsku v regionu Ida-Viru okolo města Narva na hranici s Ruskem mluví rusky 80 % obyvatelstva. Podobná situace je v okolí lotyšského města Daugavpils vzdáleného 30 km od ruské hranice, kde se 55 % obyvatelstva identifikuje jako

[46] NB8. NB8 WISE MAN REPORT. Riga, Kodaň. [online]. 2010. [cit 2022-01-14]. Dostupné z: https://vm.ee/sites/default/files/content-editors/NB8WiseMenReport.pdf?_x_tr_sl=auto&_x_tr_tl=cs&_x_tr_hl=en-US&_x_tr_pto=wapp

[47] BALTIC ASSEMBLY. *RESOLUTION of the 40th Session of the Baltic Assembly.* Vilnius, Litva. [online]. 2021. [cit. 2022-01-14]. Dostupné z https://www.baltasam.org/uploads/article-files/files/2_Resol_2021_ENGL.pdf. S. 6

rusky mluvící[48]. Právě tento faktor může vést Kreml k přesvědčení, že zmocnění se těchto území bude stejně úspěšné, jako tomu bylo v případě Krymu. Rusko se snaží o integraci s rusky mluvícími jedinci skrze výměnné pobyty studentů, stipendijní programy v rámci *Compatriot Policy*[49] nebo verbování rusky-mluvících obyvatel do proruských organizací jako je *Latvian Council of Civic Organisations* nebo *Union of Associations of the Russian Minority in Estonia*[50]. V rámci ruské reformy z roku 2002 mají všichni bývalí obyvatelé SSSR, kteří cítí historické, etnické, kulturní, jazykové i duchovní spojení s Ruskem, možnost získat ruský pas. Estonsko a Lotyšsko, díky své kulturní politice po roce 1991, totiž mají 286 300 obyvatel bez občanství.

Během roku 2021 proběhlo rozsáhlé vojenské cvičení ZAPAD-2021 ruských jednotek na hranici s Pobaltskými státy. Stále navyšující se vojenská síla Ruska zvyšuje pravděpodobnost budoucí agrese a je nezbytné zajistit připravenost států pro případný konflikt.

Rusko má stálý zájem na bývalých členech Společenství nezávislých států a stále je chce ovlivňovat. Na území Pobaltí jsou trvalé **ruské zpravodajské aktivity** snažící se narušit vnitřní pořádek, nejaktivnější jsou v oblasti okolo Kaliningradské hranice. Činnost se zaměřuje na znesnadnění role Baltských států v mezinárodních organizacích a špionáž ve strategických odvětvích. Ruská FSB, GRU i SVR pravidelně verbuje občany a především ty, kteří pravidelně navštěvují Rusko (a to i bez jejich vědomí, kdy jim při hraničních kontrolách a výsleších instalují do telefonů škodlivé softwary nebo malware). Díky pandemii COVID-19 se zároveň zvýšila kybernetické špionáž řízená FSB[51].

---

[48] M.CESARE. *Russian Encroachment in the Baltics: The Role of Russian Media and Military.* Foreign Policy Research Institute. [online]. 2020. [cit. 2021-11-16]. Dostupné z: https://www.fpri.org/article/2020/12/russian-encroachment-in-the-baltics-the-role-of-russian-media-and-military-2/

[49] A.TSATUROV. *Implications for NATO: Latvia and the Russian Hybrid Warfare Threat.* THE INTERNATIONAL AFFAIRS REVIEW. [online]. 2020. Dostupné z: https://www.iar-gwu.org/print-archive/implications-for-nato-latvia-and-the-russian-hybrid-warfare-threat. S.61

[50]FRASZKA B. *Baltic States versus Russian Hybrid Threats.* Warsaw Institute. [online]. 2020. [cit. 2022-01-30]. Dostupné z: https://warsawinstitute.org/wp-content/uploads/2020/10/BALTIC-STATES-VERSUS-RUSSIAN-HYBRID-THREATS-Bartosz-Fraszka.pdf, s.10

[51] THE CONSTITUTION PROTECTION BUREAU OF THE REPUBLIC OF LATVIA. *Our Task.* Latvia. [online]. 2022. [cit. 2022-01-22]. Dostupné z: https://www.sab.gov.lv/?a=s&id=45

Dalším prostředkem ovlivňování je **vysílání proruských zpráv** na kanálech *Russia Today (RT), First Baltic Channel (PBK), BBG* a *Sputnik TV*. Informační prostor v Pobaltí je rozdělen na dvě části: na zprávy poskytované Ruskem v ruštině a na zprávy v národních jazycích. Efektivita Ruské federace v oblasti hromadných sdělovacích prostředků je vysoká. Propaganda je mocná, fungující a dobře financovaná ze státního rozpočtu Ruska. Jejich zahraniční televize je ovlivňována nejvyššími představiteli země, aby odpovídala ruskému narativu.

Ruské programy jsou součástí televizních balíčků, a tak jsou snadno dostupné široké veřejnosti. Snaha těchto médií je zaměřena na polarizaci společnosti a znázorňování mezinárodních společenství jako nefungující instituce, které jsou rusofobní, užívající fašistické praktiky proti rusky mluvícím jedincům[52]. Ruská média jsou jednotná a navzájem se podporují se šířením dezinformací, společně tvoří image Ruska jako globální velmocí. V roce 2020 Lotyšsko a Litva zakázali vysílání RT ve spojitosti s prokremelskou propagandou. Dmitrij Kyselyov, obviněný EU za prosazování ruské propagandy ve spojení s vojenskými akcemi na Krymu, kontroloval obsah RT[53]. I přes zákaz je vliv RT je stále patrný, zaměřuje se na své webové stránky, které jsou dostupné ve všech baltských jazycích. Podporuje je i množství falešných účtů na Twitteru a Facebooku. Dalšími proruskými weby v Pobaltí jsou BaltNews a Sputnik. Tyto dva weby čerpají informační zdroje z Ruska.

V rámci boje s dezinformacemi například Estonsko spustilo na vlastní náklad ruskojazyčný program ETV+ a zřídilo web rus.err.ee.

Zvyšující se zájem na Pobaltí má také **Čína**. Její činnost se zaměřuje zejména na verbování cílových osob v rámci upevňování sociokulturních vztahů nebo vědeckých výzkumů. Bezpečnost Pobaltí je nepřímo ovlivněna situací v zemích,

[52] A.RADIN. *Hybrid Warfare in the Baltics: Threats and Potentional Responses.* RAND Corporation. Santa Monica, California. [online]. 2017.[cit. 2021-11-16] Dostupné z: apps.dtic.mil/sti/pdfs/AD1085287.pdf. s.18

[53] M.CESARE. *Russian Encroachment in the Baltics: The Role of Russian Media and Military.* Foreign Policy Research Institute. [online]. 2020. [cit. 2021-11-16]. Dostupné z: https://www.fpri.org/article/2020/12/russian-encroachment-in-the-baltics-the-role-of-russian-media-and-military-2/

kde vznikají počítače a síťový hardware (Čína) nebo software (USA). Software používaný ve vládních systémech proto může mít vliv na národní bezpečnost.

Dalšími faktory, které můžou ohrozit bezpečnost Pobaltí, jsou **energetická bezpečnostní rizika**. Rusko je stále klíčovým dodavatelem energií v Pobaltí, především elektřina je propojena systémem BRELL (Bělorusko, Rusko, Estonsko, Lotyšsko, Litva).

I přes nárůst extremistických aktivit v Evropě zůstává situace v Pobaltí stejná. Extremistická hnutí jsou málo početná a osamocená, levicový extremismus zde téměř neexistuje. Během první vlny pandemie šířily konspirační teorie, dezinformace a falešné zprávy na sociálních sítích, kde nezískali velkou podporu.

Hrozbou je taktéž pokračující **demografická krize**. Populace Pobaltí se snižuje kvůli nízké porodnosti, vysoké míře emigrace obyvatelstva do ekonomicky stabilnějších a přívětivějších zemí. Tento negativní trend je potenciální hrozbou pro politickou, ekonomickou a sociální stabilitu. Sociální a regionální vyloučení obyvatel v některých regionech dále přispívá ke zvyšování jejich nedůvěry ve státní instituce a jejich radikalizaci.

4 Estonsko

4.1 Digitalizace Estonska

Významnými sektory Estonska jsou IT, telekomunikace a bankovnictví. V roce 1994 se Estonská vláda chopila příležitosti a přidala se k užívání protokolu HTTPS (Hyper Transfer Protocol System), který zajišťuje bezpečnou komunikaci v počítačové síti. Mladá generace politiků spatřovala v používání moderních technologií možnost přechodu do moderní doby. Díky tomu, že moderní technologie a jejich užívání v každodenním životě byly na svém počátku, mělo Estonsko stejné výchozí postavení jako státy západní Evropy. V roce 1996 spustila estonská vláda projekt **e-estonia**, který započal digitalizaci veřejného sektoru. Od roku 2000 mohou občané Estonska podávat on-line daňové přiznání. V roce 2002 byl spuštěn projekt **digital ID**, kde jsou uloženy a shromážděny všechny informace o osobách (rodný list, občanský a řidičský průkaz, pas nebo kartička pojištěnce) v jednom dokumentu. V roce 2005 měli Estonci jako první země na světě možnost volit on-line[54]. Roku 2014 bylo spuštěno **e-residency**, tedy možnost stát se rezidentem Estonska online. Kdokoliv se může virtuálně stát rezidentem Estonska a založit si zde své podnikání. Tuto možnost využilo více než 16 000 společností z celého světa[55]. Občané Estonska mají centralizovaný přístup ke všem elektronickým službám a institucím na stránkách https://www.eesti.ee/et/.

Zajištění kybernetické bezpečnosti je primárním článkem Estonské společnosti. Ti, jenž se podílejí na zajištění krizových plánů, se nezaměřují na konkrétní útoky a konkrétní scénáře, ale na vytvoření detailního plánu k ochraně kritické infrastruktury. Ochrana kybernetického prostoru je docílena díky veřejnému sektoru, soukromému sektoru a dbalosti občanů, protože každý uživatel zařízení připojeného do internetové sítě, může stát potenciálně ohrozit. Uvědomělost občanů Estonska se zvyšuje jejich podílením se na *Cyber Unit of Estonian Cyber League*, která je dobrovolnou organizací zajišťující pomoc při monitorování

[54] E-ESTONIA. *i-Voting.* Estonia. [online]. 2021. [cit. 2021-11-15]. Dostupné z: https://e-estonia.com/solutions/e-governance/i-voting
[55] E-ESTONIA. *We have built a digital society and we can show you how*. Estonia. [online]. 2021. [cit. 2021-11-15]. Dostupné z: https://e-estonia.com/

kybernetického prostoru[56]. Estonská vláda také vynaloží každý rok mnoho prostředků do e-vzdělávání obyvatelstva. V největší vlně digitalizace zajistila například bezplatné počítačové kurzy pro dospělou populaci, což zvýšilo počet uživatelů internetu z 29 % v roce 2000 až na 91 % v roce 2016. Přesto je tato země velmi náchylná k tomu stát se terčem hybridního nebo kybernetického útoku. Nejvíce kybernetických incidentů se stává kvůli chybám v programech, není ale vyloučen cílený útok na kritickou infrastrukturu země, nebo dokonce vládu, jako se tomu odehrálo v roce 2007.

4.1.2 Kyberútoky v Estonsku 2007 a jejich důsledky

V dubnu roku 2007 vláda Estonska rozhodla o přestěhování sochy vojáka z centra Tallinnu na vojenský hřbitov. Tato událost vyvolala vlnu protestů u Rusů a ruských Estonců, kteří v tomto aktu spatřovali urážku a nerespektování Rudé armády, jež osvobodila Estonsko od nacismu. Ve stejný čas započal masivní kybernetický útok, který postihl celý veřejný digitální systém správy Estonska, estonské noviny, banky a emailové domény. Dne 26. dubna byl zaznamenán první kyberútok, největší silou však udeřil 9. května a prakticky skončil až 23. května. Útoky byly vedeny typy DoS (*generování požadavků s cílem zahltit systém a omezit či vyřadit služby počítačových systémů*) a DDoS (*koordinovaný útok z mnoha uzlů sítě*[57]), většinou registrovanými pod ruskými IP adresami. Zaměřily se na webové stránky všech estonských ministerstev, dvou bank a některých politických stran. Znemožnily přístup na server emailů v parlamentu, deaktivoval kreditní karty a automatické přepážky na úřadech. Do obrany Estonského kyberprostoru se zapojil CERT tým NATO včetně některých partnerů aliance jako Německo, Izrael, Slovensko, Finsko, a tak škoda, jenž po útocích vznikla, byla pravděpodobně minimální[58].

---

[56] KOOK L. *Estonian Discourse on Cyber Risk and Security Strategy.* University of Tartu and University College London. Tallinn. 2018. [cit. 2021-11-12]. 72 s. Dostupné z: digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1136&context=scholcom. S. 45-47

[57] NÚKIB. *DoS/ DDoS útoky*. GovCERT. [cit. 2021-11-12]. 4 s. Dostupné z: https://nukib.cz/download/publikace/doporuceni/Doporuceni_DDoS.pdf

[58] A. KOZLOWSKI. *Comparative Analysis Of Cyberattacks On Estonia, Georgia And Kyrgyzstan.* University of Lodz. Poland. 2013. [cit. 2021-11-12]. 10 s. Dostupné z: https://www.researchgate.net/profile/Nnedinma-Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000/International-Scientific-Forum-ISF-2013vol3.pdf#page=246. s. 237-238

Po těchto útocích Estonsko zveřejnilo jejich detaily, samotný průběh a způsob, jak jej odvrátila. Stalo se tak prvním státem, na kterém se studovala jeho schopnost efektivně zabránit útoku a v pokračování fungování digitální veřejné správy během útoku.

V roce 2008 bylo v Tallinnu založeno pod záštitou NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE). Toto centrum se zaměřuje na vytváření obranných kybernetických strategií skrze multidisciplinární mezinárodní analýzy různých kybernetických problémů, jimž mezinárodní společenství čelí. Zároveň je úkolem CCDCOE vzdělávání vojenských a civilních expertů z 21 zemí a simulace různých kybernetických útoků na vládní systémy. Jejich cílem je zajistit adekvátní reakci na ně. Nejznámějším počinem CCDCOE je *Tallinn Manual*, respektive jeho verze 2.0. Jeho obsahem je studie o mezinárodních systémech práva při obraně před kybernetickými útoky nebo neregulovanými kybernetickými operacemi[59].

4.2 Bezpečnostní strategie Estonska – instituce

Bezpečnostní situaci Estonska monitoruje a zajišťuje mnoho státních nebo mezinárodních institucí. Velmi důležitým článkem jsou však i samotní obyvatelé, kteří jsou povinni bránit nezávislost státu. Vláda napomáhá zajišťovat bezpečnost ve státě. Pro lepší efektivitu zřizuje **Bezpečnostní výbor** (*Vabariigi Valitsuse julgeolekukomisjon*), který koordinuje činnost bezpečnostních složek, vojenského zpravodajství, orgány výkonné moci při plánování, rozvoji a organizaci obrany státu. Stanovuje také akční plány při obraně státu, vyhodnocuje rizika a schopnost integrované obrany státu. Jeho činnost se řídí National Defence Act. V rámci bezpečnostního výboru byl v roce 2006 založen **Cyber Security Council**. Spolupracuje a dohlíží na plnění cílů, které jsou vytyčeny Strategií kybernetické bezpečnosti 2019-2022[60].

[59] CCDCOE. *About Us.* NATO. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://ccdcoe.org/about-us/

[60] VLÁDA ESTONSKA. *Riigikaitseseadus*. Estonia. [online]. 2015. [cit. 2022-01-21]. Dostupné z: https://www.riigiteataja.ee/en/eli/502042019010/consolide

CERT-EE je útvarem Odboru kybernetické bezpečnosti úřadu pro informační systém. Je financován ze státního rozpočtu. Jeho cílem je zajištění kybernetické bezpečnosti, ochrana a dohled nad kritickou infrastrukturou[61].

Další institucí je **Rada obrany státu** (*Riigikaitsekomisjon*), tvořená prezidentem estonského parlamentu *Riigikogu*, premiérem, předsedy Národního výboru pro obranu a zahraničního výboru, ministry obrany a velitelem ozbrojených sil. Je poradním orgánem prezidenta Estonska. Hlavní činností orgánu je vykonávat vládní dohled nad vytvářením bezpečnostní politiky státu, včetně vytváření zákonů[62].

The International Centre for Defence and Security (*Rahvusvaheline Kaitseuuringute Keskus*) je think-thank pod záštitou Estonské vlády. Jeho cílem je posilovat bezpečnostní a obranný sektor Estonska, vylepšit bezpečnostní strategii Pobaltí v rámci EU a NATO skrze analýzy, doporučení a zvyšování povědomí veřejnosti o bezpečnosti. Jeho cílem je osvěta – pořádá mnoho konferencí, mimo jiné každoroční Baltic Conference on Defence[63].

Významnými jsou zpravodajské služby. Za činnost odpovídá a koordinuje ji vláda. **KaPo** (*Kaitsepolitseiamet*), vnitřní rozvědka, shromažďuje informace, předchází a zabraňuje zpravodajské činnosti jiných států na území Estonska proti jeho zájmům, je zde pro prevenci a boji proti terorismu nebo korupci. Především chrání státní tajemství před cizími vlivy. Svá zjištění zveřejňuje ve výročních zprávách[64]. **Välisluureamet**, vnější rozvědná služba, je povinna shromažďovat, předkládat a vyhodnocovat informace o vnějších hrozbách. Je první linií mezinárodní ochrany se svým systémem včasného varování před nenadálými hrozbami. Chrání Estonské diplomaty nebo vojáky v zahraničí. Pro svou činnost využívá všechny

[61] REPUBLIC OF ESTONIA: INFORMATION SYSTEM AUTHORITY. *RFC 2350 Description for CERT-EE.* [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.ria.ee/en/cyber-security/cert-ee/rfc-2350.html

[62] PARLIAMENT OF ESTONIA. *The National Defence Committee.* [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.riigikogu.ee/en/parliament-of-estonia/committees/national-defence-committee/introduction/

[63] ICDS. *About ICDS.* Estonia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://icds.ee/en/about/

[64] KAITSEPOLITSEIAMET. *General Information.* Estonsko. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://kapo.ee/en/content/general-information-0/

zpravodajské větve HUMINT, SIGING, IMINT i OSINT[65]. **Kaitseväe Luurekeskus** je estonským vojenským zpravodajstvím. Zpracovává informace pro vojenskou obranu státu, připravuje podklady pro mezinárodní vojenské operace a předchází cizí zpravodajské činnosti. Zároveň poskytuje bezpečnostní prověrky.

Resortem v rámci vlády, který se zabývá bezpečnostní otázkou, je **Ministerstvo vnitra** (MV). Stará se o domácí i zahraniční politiku, vnitřní pořádek a bezpečnost. Pod MV můžeme řadit činnost **estonské policie** (*Eesti Politsei*) a **výbor pohraniční stráže Estonska** (*Politsei-ja Piirivalveamet*), jehož fungování zajišťuje okolo 6500 osob, včetně dobrovolníků. Oba tyto policejní orgány vydávají osobní doklady a víza, hlídají hranice nebo situaci na moři. Její činnost se díky rozsáhlé digitalizaci Estonska rozšiřuje na vyšetřování kybernetických trestných činů[66].

Neopomenutelnou institucí, jenž se zajišťuje o celkovou bezpečnost je **Estonská armáda** (*Maavägi)*. Je tvořena **pozemní armádou**, **námořnictvem** a **vzdušnými silami**. V současné době má přibližně 6 600 vojáků z povolání, 4 000 v doplňkové rezervě a dalších 16 000 jich je v aktivních zálohách. V rámci NATO vydává Estonsko 2,13 % ze svého HDP do jeho rozpočtu.

4.3 Bezpečnostní strategie – základní dokumenty a cíle

K zajištění efektivní a funkční obrany země je nutné, aby Estonsko stavělo na pilířích vojenské obrany, podpory civilního sektoru k chodu vojska, kvalitní mezinárodní diplomacii, mezinárodní bezpečnosti, schopných institucí a psychologické obrany[67]. Estonsko by se mělo zaměřit na identifikaci nepřátelských hrozeb, které by mohly zeslabit národní obranu, průběžně upozorňovat obyvatelstvo na případné ohrožení a připravit scénáře pro krizové situace.

[65] VALISLUUREAMET. *Estonian Foreign Intelligence Service public report 2021*. Estonia. [online]. 2021. [cit. 2021-11-12]. Dostupné z: https://www.valisluureamet.ee/en.html
[66] ESTONIAN POLICE AND BORDER GUARD BOARD. *The Story and Values.* Estonia. [online]. 2021. [cit. 2021-11-12]. Dostupné z: https://www.politsei.ee/en/the-story-and-values
[67] ESTONIAN MINISTRY OF DEFENCE. *National Defence Strategy*. Estonia. [online]. 2011. [cit. 2021-11-12]. 28 s. Dostupné z: https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf . S.10

4.3.1 National Security Concept of the Republic of Estonia *(Eesti julgeolekupoliitika alused)*

Základním dokumentem pro estonskou bezpečnostní politiku je Národní bezpečnostní koncept z roku 2017. Byl vypracován dle pokynů Estonské vlády a následně jej schválil Parlament, *Riigikogu*. Jeho cílem je implementovat navržené změny v bezpečnostní sféře a každé dva roky hodnotit, zda toho bylo úspěšně docíleno. Koncept je rozdělen do 3 částí, tedy na cíle bezpečnostní politiky a zásady pro jejich realizaci, bezpečnostní prostředí a cíle a pokyny k jejich realizaci. Národní bezpečnostní situace přímo souvisí s digitálními službami, které jsou v Estonsku na velmi vyspělé úrovni a jsou široce propojeny. Vyřazení nebo napadení jednoho systému by mělo za následek rozsáhlé škody. Koncept je apelem na spolupráci mezi státními institucemi, včetně těch mezinárodních, a na začlenění všech článků společnosti, aby se takovým situacím zabránilo. Hodnotí současnou bezpečnostní situaci, která je ovlivněna zejména ruským vyzbrojováním v těsné blízkosti Estonska a celého Pobaltí, tedy nárazníku mezi NATO a východním světem. Je důležité, aby celý Baltský region zajišťoval silnou kontrolu na jeho vnějších hranicích kvůli předcházení mezinárodnímu nebezpečí.

Ekonomická bezpečnost a infrastruktura je zajištěna investicemi do klíčových sektorů a rozvoje IT systémů. Estonsko musí mít přehled nad komunikačními systémy a touto infrastrukturou, včetně zálohování a duplikování dat k jejich zabezpečení proti případnému zneužití či útoku. Estonský kyberprostor závisí na expertech a samotných uživatelích, a proto je nezbytné zajišťovat jejich pravidelné vzdělávání.

Odolnost a soudržnost společnosti je další prioritou. Cílem je zlepšit strategickou komunikaci s veřejností a zajistit soudržnost obyvatel, i skrze jejich zapojení do vytváření bezpečného prostředí. Bipolarita národa na ruskou a estonskou část má negativní vliv na stát. Je proto nezbytné, aby se tyto dvě národnosti sjednotily a společně se podílely na rozvoji země. Estonsko nesmí rozlišovat a musí zajistit, aby chránilo hodnoty všech svých obyvatel rovnocenně. Důležitá je kooperace mezi státem, místními samosprávnými celky, soukromým sektorem a veřejností. Zároveň je důležité, aby do budoucna obyvatelé věděli, jak reagovat na potenciální nebezpečí. Budou se pořádat cvičení bezpečnostních složek za účasti

obyvatelstva Estonska. Tato celonárodní cvičení pomůžou v budoucnosti zvládat krize[68].

4.3.2 Cybersecurity Strategy 2019-2022

Cybersecurity Strategy je dokumentem vyhodnocujícím současnou estonskou kybernetickou bezpečnost. Cílem tohoto dokumentu je poskytnout rady a implementovat je ve 3 klíčových oblastech: kritická infrastruktura a životně důležité služby, kybernetický zločin a národní obrana. Řídí se čtyřmi principy, především ochranou a prosazováním základních práv a svobod i v rámci kybernetického prostoru, podporou inovací v bezpečnostním sektoru, bezpečnou kryptografií a transpare ntností. Prioritami jsou vývoj nových služeb v oblasti bezpečnosti (autorizovaný monitoring a testování bezpečnosti sítě kritické infrastruktury), efektivní spolupráce na ose stát – akademická sféra – soukromý sektor, analýza nových trendů a rizik (zajištění schopnosti rychlé reakce), inovace a vzdělávání občanů v oblasti kybernetiky[69].

4.3.3 Estonian Foreign Policy Strategy 2030

Estonsko má zájem na globální prosperitě, protože malé země se musí více spoléhat na členství v mezinárodních společenstvích. Je známé e-governmentem, digitální identitou občanů, e-službami a kybernetickým zabezpečením země. Nejpodstatnějším cílem vytyčeným ve Strategii estonské zahraniční politiky je podílení se na založení a posílení kybernetické iniciativy v EU, NATO, OSN, nebo OSCE. Spolupráce s mezinárodními organizacemi bude do budoucna oboustranně benefitní[70].

---

[68] RIIGIKOGU. *National Security Concept 2017.* Estonia. [online]. 2017. [cit. 2022-01-21]. 22 s. Dostupné z: https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf

[69] REPUBLIC OF ESTONIA: MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS. *Cybersecurity Strategy 2019-2022.* [online]. 2019. [cit. 2022-01-23]. 71 s. Dostupné z: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[70] REPUBLIC OF ESTONIA: MINISTRY OF FOREIGN AFFAIRS. *Estonian Foreign Policy Strategy 2030.* Tallinn. [online]. 2020. [cit. 2022-01-23]. 42 s. Dostupné z: https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/estonian_foreign_policy_strategy_2030_final.pdf#:~:text=The%20Foreign%20Policy%20Strategy%20has%20been%20drawn%20up,of%20Estonia%E2%80%99s%20inter-%20ests%20in%20a%20changing%20environment.

5 Lotyšsko

5.1 Digitalizace Lotyšska

Podobnou úroveň a rozsah digitalizace má po Estonsku také Lotyšsko. V roce 2018 zahájil Úřad pro záležitosti občanství a migrace modernizaci projektu *Data Service*. Jeho cílem je rozvoj informačního systému státu, včetně zavedení povinného e-ID, tedy digitální identity osob pro všechny obyvatele[71]. Občané Lotyšska mají centralizovaný přístup ke všem elektronickým službám a institucím na stránkách https://latvija.lv/ a pomocí elektronické identity nebo podpisu mohou vyřizovat záležitosti s úřady online. Stát zavedl několik programů podpory inovace a digitalizace ve firmách, která se díky pandemii velmi urychlila. V roce 2021 mělo 91 %[72] obyvatel Lotyšska internet v domácnosti.

5.2 Bezpečnostní strategie Lotyšsko – instituce

Sjednocování bezpečnostní politiky, dohled a plánování vypracování základních bezpečnostních dokumentů zabezpečuje **Národní bezpečnostní rada Lotyšska** (*Nacionālās drošības padome*). Je součástí prezidentova kabinetu, členy jsou předseda parlamentu (*Saeima*), předsedové stálých výborů Saeima pro národní bezpečnost a obranu, premiér, ministři obrany, zahraničních věcí a vnitra[73].

CERT.lv je institucí, která reaguje na bezpečnostní incidenty v kybernetickém prostoru Lotyšska. Působí pod ministerstvem obrany a jejími hlavními úkoly je informovat o bezpečnostních hrozbách, poskytovat rady státním institucím, organizovat vzdělávací programy pro odborníky, ale i veřejnost[74]. Podporu

[71] EUROPEAN COMMISION. *Digital Government Factsheet 2019 Latvia*. Latvia. [online]. 2019. [cit. 2022-01-23]. 45 s. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Latvia_2019.pdf, s. 6

[72] OFFICIAL STATISTICS PORTAL. *Access of Internet by households.* Latvia. [online]. 2022, [cit. 2022-01-23]. Dostupné z: https://stat.gov.lv/en/statistics-themes/information-technologies/computers-and-internet/5675-access-internet-households?themeCode=DL

[73] VALSTS PREZIDENTA KANCELEJA. *National Security Council.* Latvia. [online]. 2021. [cit. 2022-01-23]. Dostupné z: https://www.president.lv/en/national-security-council

[74] CERT.LV. *About Us.* Latvia. [online]. 2022. [cit. 23.01.2022]. Dostupné z: https://cert.lv/en/about-us

CERT.lv zajišťuje **Cyber Defence Unit**, v podobě informací nebo podpory jednotkám národních ozbrojených sil v případě krize[75].

Bezpečnostní složky Lotyšska zahrnují také **policii** *(Valsts Policija).* Dle Lotyšského zákona o policii *je ozbrojenou militarizovanou státní institucí chránící základní společenské hodnoty a předcházející protiprávnímu jednání*.[76]

Valsts drošības dienests, čili Služba vnitřní bezpečnosti, shromažďuje veškeré informace o potencionálních hrozbách, které by mohly narušit národní bezpečnost. Činnost také zahrnuje přijímání opatření k prosazení obrany státu, ochrany státního tajemství a dalších, jako jsou obrana proti korupci, terorismu, apod[77]. **Satversmes aizsardzības birojs**, tedy Úřad pro ochranu ústavy zajišťuje zpravodajskou a kontrarozvědnou činnost v zahraničí, ochranu utajovaných informací institucí Lotyšska, ale i NATO a EU. Identifikuje hrozby a analyzuje poznatky týkající se jak politické, tak ekonomické situace nebo vojenských aktivit[78]. **Militārās izlūkošanas un drošības dienests**, Obranná zpravodajská služba je vojenskou rozvědkou podřízenou ministerstvu obrany (MO). Jejími úkoly jsou rozvědná a kontrarozvědná činnost, ochrana státního a vojenského obranného tajemství, mimo jiné také udělování a prověřování licencí vydaných MO[79]. Všechny tyto zpravodajské služby spolu úzce spolupracují.

Armáda (*Latvijas Nacionālie bruņotie spēki*) je tvořena pozemními silami, námořnictvem, vzdušnými silami (6 900 vojáků), dobrovolnickou Litevskou národní gardou (*Latvijas Republikas Zemessardze*; 8 000 členů) a (o počtu 6 000 členů). Kooperují nejen s ostatními bezpečnostními jednotkami státu, jejich fungování je založeno na vojensko-civilní spolupráci. V rámci NATO vydává Lotyšsko 2,01 % ze svého HDP do jeho rozpočtu.

---

[75] MINISTRY OF DEFENCE. *CDU Concept.* Latvia. [online]. 2013. [cit. 2022-01-23]. 8 s. Dostupné z: https://www.mod.gov.lv/sites/mod/files/document/cyberzs_April_2013_EN_final.pdf

[76] SUPREME COUNCIL. *About the Police.* Latvia. [online]. 1991. [cit. 2022-01-21]. Dostupné z: https://likumi.lv/doc.php?id=67957

[77] VALSTS DROŠĪBAS DIENESTS. *About Us.* Latvia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://vdd.gov.lv/en/about/about-us

[78] THE CONSTITUTION PROTECTION BUREAU OF THE REPUBLIC OF LATVIA. *Our Task.* Latvia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://www.sab.gov.lv/?a=s&id=45

[79] MILITĀRĀS IZLŪKOŠANAS UN DROŠĪBAS DIENESTS. *About Us.* Latvia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://midd.gov.lv/en/about-us

NATO Strategic Communications Centre of Excellence (StratCom COE) bylo založeno v Rize v roce 2014 s cílem zlepšit strategickou komunikaci v rámci NATO a spojeneckých zemí. StratCom COE se věnuje rozvoji mezinárodní politiky, vývoji metod výcviku skrze simulace dezinformačních útoků nebo kurzy a konference o sociálních sítích a vzdělávání[80].

5.3 Bezpečnostní strategie – základní dokumenty

5.3.1 The National Security Concept *(Valsts Aizsardzības Koncepcija)*

Koncept národní bezpečnosti byl zpracován jako analýza současných hrozeb ohrožujících Lotyšsko s cílem vytyčit priority pro jejich předcházení. Podporuje komplexní systém obrany státu. Hrozby rozděluje do sedmi oblastí, tedy na vojenské, kybernetické, hospodářské hrozby, zahraniční zpravodajské či bezpečnostní služby, ohrožení vnitřní bezpečnosti a ústavního systému, ohrožení lotyšského kybernetického prostoru a hrozby týkající se mezinárodního terorismu. Národní bezpečnostní politika musí být jednotná a směřovat k efektivnímu odhalování, prevenci a překonání hrozeb díky kooperaci všech lotyšských institucí a aktivní participaci v mezinárodních společenstvích. Být členy NATO a EU je pro Lotyšsko zásadní. Zabezpečit stát před hrozbami ohrožující vnitřní uspořádání lze díky zesílení obrany na hranicích, především vnějších hranicích (zvýšením počtu stráží a obnovením jejich techniky). Je nutné zlepšit a zvýšit kvalitu bezpečnostních složek státu jejich společným výcvikem. Vedoucí jednotlivých složek musí být důkladně vyškoleni na kooperaci v případě krizové situace. Lotyšsko také bude do budoucna posilovat civilně vojenskou spolupráci. Posledním důležitým krokem je monitoring a preventivní opatření před radikalizací obyvatelstva. Vláda Lotyšska by měla zajistit vzdělání pro občany a posilovat jejich národní smýšlení. Zajištěním kontrarozvědné obrany před zahraničními zpravodajskými službami operujícími na území Lotyšska lze posílit národní bezpečnostní politiku. Je nutné dbát na pečlivou analytickou činnost, přizpůsobení se novým typům hrozeb, využívat nové technologie, systematickou výměnu informací, a především kooperaci vnitřních bezpečnostních složek.

[80] NATO STRATCOM COE. *About NATO StratCom COE.* Riga. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

Hrozby v kybernetickém prostoru se zvyšují kvůli nedostatku znalostí digitální hygieny koncových uživatelů v soukromém i státním sektoru. Dalším faktorem je nedostatek IT specialistů, kteří Lotyšsko opouštějí kvůli lepším platovým podmínkám v zahraničí. Orgány činné v trestním řízení nemají dostatečně upravenou legislativu a kapacity na řešení kybernetické kriminality. Cílem tohoto plánu je efektivní kybernetická bezpečnostní politika, tedy posílení schopnosti identifikace a reakce na hrozby či případná rizika. Společnost musí být vzdělávána o správném chování v kybernetickém prostoru, důležitá je spolupráce veřejnosti s CERT.lv[81].

5.3.2 Comprehensive National Defence in Latvia 2020 (CND)

Plán vytvořený lotyšským Ministerstvem obrany by se měl přizpůsobovat neustále se měnící bezpečnostní situaci a hrozbám. Zajišťuje bezpečnostní a krizovou připravenost napříč všemi sektory společnosti. Navrhovanými aktivitami jsou například kurzy státního uvědomění ve školách a zvyšování povědomí lotyšských obyvatel o státotvorbě. Výuka by měla podporovat kritické myšlení a patriotismus. Studenti musí mít možnost diskutovat přímo o národní obraně, může to pomoci prohloubit porozumění o výzvách státu. Civilní obrana a vytváření krizového plánu, psychologické obrana nebo strategická komunikace pomůže prohloubit vazby soukromého a vládního sektoru pro případ krize. Ekonomická odolnost by měla být zaručena vytvořením krizového ekonomického plánu. Zároveň stát musí zajistit rezervy komodit pro případ nefunkčnosti státu. Cílem jsou konkrétní úkoly pro veřejné orgány, rámcové plánování a rozhodování v případě krize, nebo schopnost Lotyšského obyvatelstva reagovat na krizové stavy[82].

5.3.3 National Development Plan of Latvia for 2021-2027

Národní plán rozvoje schválený parlamentem Saeima obsahuje 8 oblastí, na které se má Lotyšsko v budoucnosti zaměřit. Prioritami jsou sociální spravedlnost, regionální rozvoj, vybudování infrastruktury pro dodávky energií, energetický

[81] AIZSARDZĪBAS MINISTRIJA. *The National Security Concept.* Latvia. [online]. 2020. [cit. 2022-01-23]. 29 s. Dostupné z: https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf

[82] AIZSARDZĪBAS MINISTRIJA. *Comprehensive National Defence in Latvia.* [online]. 2020. [cit. 2022-01-23]. 7 s. Dostupné z: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mod.gov.lv%2Fsites%2Fmod%2Ffiles%2Fdocument%2FComprehensive%2520National%2520Defence%2520in%2520Latvia.docx&wdOrigin=BROWSELINK

management a jeho zabezpečení, nebo hlubší integrace v mezinárodních společenství. Lotyšsko je po Estonsku státem, který má většinu svých veřejných služeb online. Do budoucna je pro Lotyšsko výzvou zajistit větší integraci digitálních technologií do běžného života. Zároveň je nutné, aby se předcházelo počítačové kriminalitě a včasně se posuzovala kybernetická bezpečnostní rizika. Plán se zaměřuje na prevenci, schopnost samotných obyvatel adekvátně a efektivně reagovat na útoky a také jejich spolupráci s dalšími články společnosti[83].

5.3.4 Latvian Counter-Terrorism Strategy 2021-2026

Dle analýzy současných teroristických trendů a hrozeb byla vypracována Státní bezpečnostní službou (VDD) protiteroristická analýza. Mezi její priority staví mezinárodní kooperaci. Cílem plánu je zajistit prevenci před radikalizací a násilným extremismem, zlepšení ochrany měkkých a tvrdých objektů, úprava předpisů a protiteroristických akčních plánů. Je nutné zajistit připravenost institucí, které jsou zapojeny do protiteroristických opatření a podpora veřejnosti na účasti při čelení hrozbám[84].

[83] CROSS-SECTORAL COORDINATION CENTER. *National Development Plan of Latvia for 2021-2027*. Riga. [online]. 2020. [cit. 2022-01-23]. 89 s. Dostupné z: https://www.pkc.gov.lv/sites/default/files/inline-files/NAP2027__ENG.pdf

[84] MINISTRY OF THE INTERIOR. *Latvian counter-terrorism strategy developed by the State Security Service approved.* [online]. 2021. [cit. 2022-01-24]. Dostupné z: https://www.iem.gov.lv/en/article/latvian-counter-terrorism-strategy-developed-state-security-service-approved

6 Litva

6.1 Hybridní působení a bezpečnostní hrozby v Litvě

Díky celosvětové pandemii spustila Čína masovou propagandu zaměřenou především na diplomacii. Zajistila, aby veškeré dodávky zdravotnického materiálu byly z Číny, postavila se do role globálního vůdce a zdůraznila nedostatek solidarity mezi demokratickými zeměmi. Dodávky do Litvy veřejně vykreslila jako pomoc od svých společností se sídly v této zemi, které mají přímé zájmy v telekomunikacích a energetickém průmyslu.

Velmi kritický je pro Litvu vztah s Běloruskem. Politická krize v Bělorusku se odráží také na bezpečnostní situaci Litvy. Po zmanipulovaných volbách v Bělorusku se Litva postavila na stranu opozice a podpořila Tsikhanouskayovou. Také jí byl poskytnut politický azyl. Během května roku 2021 byli 2 běloruští diplomaté z ambasády v Litvě, členové zahraniční zpravodajské služby[85]. Během roku 2021 vznikla migrační krize na hranicích s Běloruskem. Prezident Lukašenko otevřel, na protest proti EU, zemi migrantům a hrozil jejich vpuštěním do sousedních států. Polsko, Litva a Lotyšsko vyhlásili výjimečný stav na svých hranicích a vymezili se postavit hraniční zdi. Kvůli této zhoršující se situaci a vazbám na EU Bělorusko uvalilo na Litvu (i Lotyšsko) sankce týkající se snížení počtu diplomatů Litvy (Lotyšska) na jejím území[86]. Dalším ohrožením bezpečnostní situace v Litvě bylo spuštění běloruské jaderné elektrárny bez dokončení patřičných systémových testů[87]. Bělorusko se v neposlední řadě snaží o podvrácení země skrze verbování litevských občanů do KGB.

Zvýšil se také počet kybernetických útoků proti Litvě. Rok 2020 je spojen s šířením dezinformací zajišťující diskreditaci Litvy a státních institucí před jejími občany.

[85] ADAMI M. *Lithuania expels two Belarusian diplomats*. Politico. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.politico.eu/article/lithuania-expels-two-belarusian-diplomats/
[86] HERSZENHORN D.M. . *Belarus expels Lithuanian diplomats as ties with EU crumble.* Politico. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.politico.eu/article/belarus-expels-diplomats-as-ties-with-eu-crumble/
[87] LRT. *Secrecy'at Belarus nuclear plant a danger to Lithuania – intelligence*. Lithuania. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.lrt.lt/en/news-in-english/19/1358172/secrecy-at-belarus-nuclear-plant-a-danger-to-lithuania-intelligence

Celkově bylo během toho roku zaznamenáno 9 takových, velmi rozsáhlých kybernetických operací[88].

6.3 Bezpečnostní strategie Litvy – instituce

Valstybės gynimo taryba (State Defence Council), jehož hlavou je prezident, projednává a koordinuje zajištění bezpečnosti a obrany státu, včetně řešení bezpečnostních otázek. Členy jsou premiér, předseda Saeima, ministr národní obrany a velitel ozbrojených sil[89].

Nacionalinis kibernetinio saugumo centras (National Cyber Security Centre) zřízené pod ministerstvem národní obrany Litvy bylo založeno v roce 2018 za účelem národní ochrany kybernetického prostoru a výzkumu kybernetické bezpečnosti. Toto centrum sdružuje nahlášené incidenty v kyberprostoru a provádí jejich analýzu[90]. Další podobnou institucí je **LITNET CERT** zabývající se především bezpečnostními problémy v oblasti IT. Hlavní činností je poskytování informací o hrozbách a koordinace protiútoků[91].

Valstybes saugumo departamentas (State Security Department) shromažďuje informace, které se týkají vnitřní bezpečnosti Litvy. Je kontrarozvědnou a zpravodajskou institucí, chrání státní tajemství a předchází jeho zneužití apod. Je jedinou litevskou civilní zpravodajskou službou. O své činnosti vydává každoroční hodnocení bezpečnostních rizik. Vojenské zpravodajství je zajišťováno **Antrasis operatyvinių tarnybų departamentas** (Second Investigation Department)[92].

---

[88] STATE SECURITY DEPARTMENT OF THE LITHUANIA AND DEFENCE INTELLIGENCE AND SECURITY SERVICE UNDER THE MINISTRY OF NATIONAL DEFENCE. *National Threat Assessment 2021*. Lithuania. [online]. 2021. [cit. 2022-01-03]. 78 s. ISSN 2669-2732. Dostupné z: https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf . s. 15, 18-23, 41-43, 46-47

[89] REPUBLIC OF LITHUANIA. *Law on the Basics of National Security*. [online]. 1997. [cit. 2022-01-20]. 25 CH. Dostupné z: https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=9tq147ume&documentId=TAIS.39790&category=TAD. H16

[90] NSCS. *About Us.* Lithuania. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://www.nksc.lt/en/structure.html

[91] LITNET CERT. *About.* Lithuania. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://cert.litnet.lt/about/

[92] STATE SECURITY DEPARTMENT OF LITHUANIA. *Intelligence*. Lithuania. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.vsd.lt/en/activities/intelligence/

Litevská **armáda** (*Lietuvos ginkluotosios pajėgos*) se skládá z pozemních a vzdušných sil, námořnictva, speciálních operačních sil a dobrovolníků v rezervách. Činnost je koordinována ministerstvem obrany a cílem je udržení státní suverenity, stability a všeobecné ochrany[93]. Celkem je vojsko tvořeno 20 000 vojáky a dalšími 90 000 osobami v aktivní záloze. V rámci NATO vydává Litva téměř 2 % ze svého HDP do jeho rozpočtu.

Policie (*Lietuvos Policijos pajegos*) je jednotným orgánem pod ministerstvem vnitra a dalším článkem litevských bezpečnostních služeb. Její jednotky zajišťují ochranu zákona, analýzu informací a další obvyklé policejní činnosti.

6.4 Bezpečnostní strategie – základní dokumenty

6.4.1 National Security Strategy of Lithuania

Základními vytyčenými prioritami pro zajištění bezpečnosti Litvy jsou navýšení rozpočtu pro obranu, zvýšení počtu osob ve vojenských zálohách, vývoj systému pro rozpoznání. Dále pak je to posouzení a upozornění na hrozby nebo nebezpečí, které by mohly ohrozit národní bezpečnost. Obyvatelstvo Litvy musí být připraveno bránit se během míru i války. Je proto nutné posílit civilní obranu. Posílením civilní ochrany a veřejné bezpečnosti lze zajistit preventivní opatření pro předcházení zločinu a radikalismu. Tímto způsobem se také může zajistit ochrana vnějších hranic se státy mimo EU. Litva musí do budoucna vyvinout systém identifikace nebezpečných situací a hrozeb společně s organizací, která by poskytla okamžitou pomoc v krizi.

Podle tohoto plánu je nutné zajistit informační bezpečnost Litvy. Cílem musí být zajištění implementace prostředků proti hybridnímu působení na politické, finanční nebo informační instituce. Pro všechny Baltské státy je důležité plně se podílet na posílení přípravy NATO a jeho krizového managementu. Je nutná aktivní spolupráce členských států a jejich sdílení nejlepších zkušeností z praxe. Stát musí zajistit ochranu kritické infrastruktury a strategického průmyslu pomocí vyvinutí národního kybernetického bezpečnostního systému a kooperaci státního,

[93] LITHUANIAN ARMED FORCE. *Who are we?* Lithuania. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.kariuomene.lt/en/who-we-are/military-service/23649

civilních a nevládních sektorů[94]. V návaznosti na Národní bezpečnostní strategii byla vytvořena *Lithuania's Progress Strategy "Lithuania 2030",* jejíž cílem je dlouhodobé zajištění plynulého rozvoje státu, posílení základních hodnot, podpora inovací v oblasti společnosti, ekonomiky a vládnutí.

6.4.2 National Cyber Security Strategy

Cílem této Strategie schválené v roce 2018 je vytyčit hlavní směr národní kybernetické bezpečnostní politiky. Priority jsou shrnuty do 5 částí: *schopnosti státu zabezpečit kybernetickou obranu, předcházet trestným činům v kyberprostoru, implementace inovací, kooperace soukromého a veřejného sektoru* a *mezinárodní spolupráce.* Stát se stará o rozvoj kybernetické bezpečnosti a prevenci. Vytváří komplexní plány pro situace ohrožení, informuje veřejnost, vytváří mapy a scénáře typických rizik pro jednotlivá odvětví. Pro snížení administrativní zátěže při těchto procesech je nutné upravit legislativu, analyzovat dobré praktiky a ustanovit aktuální národní krizový plán. Zločin v kybernetickém prostoru lze vyšetřovat jen za předpokladu plné spolupráce orgánů činných v trestním řízení, vzdělávacích institucí a veřejnosti. Zajištěním plné spolupráce soukromého a veřejného sektoru pomocí systému včasného varování, výměny informací a odhalováním mezer v zabezpečení, lze dosáhnout bezpečnějšího kybernetického prostoru. Kyberprostor je neohraničený, a tak je národní bezpečnost ovlivněna situací ve světě. Pro Litvu je nutná aktivní spolupráce včetně prohlubování vztahů s mezinárodními organizacemi[95].

[94] SEIMAS OF THE REPUBLIC OF LITHUANIA. *National Security Strategy.* Lituhania. [online]. 2017. [cit. 2022-01-21]. ISBN 978-609-412-113-5. 20 s. Dostupné z: https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf

[95] GOVERNMENT OF THE REPUBLIC OF LITHUANIA. *National Cyber Security Strategy.* [online]. 2018. [cit. 2022-01-25]. 20 s. Dostupné z: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

7 Státní bezpečnostní agenda ČR v komparaci s Pobaltskými státy

7.1 Digitalizace a kybernetická obrana

Česká republika je v porovnání s Baltskými státy velmi zaostalá v digitalizaci. Estonsko se svou bezpapírovou administrativou vynaloží celkem 1 % HDP do zabezpečení a provozu digitálních systémů ročně, zároveň ale 2 % HDP ušetří. Díky tomu poklesla korupce téměř na minimum (index vnímání korupce je zde 17 CPI dle Transparency International, v ČR 49 CPI), průhlednost o transakcích brání úplatnosti úředníků. Estonsko je velmi transparentní a nabízí ostatním státům pomoc a rady, jak docílit digitalizace. Česká vláda by se měla co nejdříve zaměřit na plnou digitalizaci veřejné správy a nechat se inspirovat, třeba právě Estonskem. Skutečně se také musí řídit radami, které jsou vytyčeny v Národní strategii kybernetické bezpečnosti 2021-2025 a každý rok zhodnocovat, zda jsou převedeny vytyčené body do praxe. Je nutné investovat do vzdělávání obyvatelstva v oblasti internetové a mediální gramotnosti, především upravit školní osnovy, aby odpovídaly potřebám 21. století. Obyvatelstvu se musí poskytnout možnost bezplatných vzdělávacích počítačových kurzů, stejně jako v Estonsku a Lotyšsku. Zároveň je nutné alokovat finance pro zabezpečení digitální architektury a pro tvorbu plně funkčního modelu k zajištění kybernetické obrany ČR. Všechna digitalizovaná data je nutné zálohovat, nejlépe je duplikovat a zabezpečit v jiném státě, aby se předešlo jejich případné ztrátě. Je důležité zajistit autorizovaný monitoring a testování sítě pomocí cílených útoků a zajistit adekvátní administrátorskou podporu a spolupráci s odborníky. Česká republika by měla do své národní strategie kybernetické bezpečnosti převzít z estonské Cybersecurity Strategy některé postupy. Zaměřit by se především měla na zajištění fungujícího systému v případě napadení kritické infrastruktury a životně důležitých služeb. V případě takových kybernetických útoků musí státy a napadené instituce spolupracovat v rámci vytyčeného plánu s národními CERT týmy a se svými kybernetickými centry.

Působení hybridního charakteru se může projevit i při využívání moderních technologií, například 5G sítí a umělé inteligence, které pocházejí ze zemí

s odlišným ideologickým směrem. Státní instituce musí zhodnocovat rizika při výběru software a digitálních zařízení. Například Litva během roku 2021 zjistila, že Čína v rámci poskytování služeb společnostmi Huawei a Xiaomi cenzoruje některé pojmy, jako je *„free Tibet“* nebo *„democratic movement“*[96]. Je nutné, aby zprostředkování nových digitálních technologií ze států s odlišnými ideovými hodnotami nezasahovalo do základních principů demokratických států. Národní bezpečnostní situace závisí přímo na digitálních službách. V případech vlivu jiných států skrze digitální technologie a služby je nutná úzká spolupráce s EU, která zajistí ochranu před tímto jednáním.

7.2 Dezinformace

Dezinformační média v Pobaltí cílí především na ruskou menšinu skrze televizi. Kabelové televize nabízí základní balíčky s mnoha ruskými kanály, jejichž obsah je kontrolován vládou Ruska. Jejich cílem je ovlivňovat společnost skrze přetváření historických událostí, narušování demokratických zájmů pomocí zpochybňování jednotlivých institucí. Dalším terčem jsou mezinárodní společenství, která jsou považována za diktaturní. Jednotlivé státy se snaží konkurovat těmto kanálům skrze spouštění svých vlastních programů v ruštině. Dále při porušování objektivního zpravodajství postihují provozovatele kanálů pokutami, případně pozastavením činnosti. Institucí, která se zabývá studiem ruské strategické dezinformační kampaně, je již zmíněný NATO StratCom COE. StratCom aktivně bojuje proti propagandě pomocí uvádění faktů. Představitelé NATO také ustanovili a vytvořili podpůrné týmy, které poskytují cílenou pomoc spojencům při čelení dezinformacím a hybridním útokům. Je nutné klást důraz na strategickou komunikaci ze strany státních institucí. Jejich marketing by se měl co nejrychleji přeorientovat na účelné plánování a budování reputace pomocí správných komunikačních kanálů[97]. Sociální sítě by měly být využívány

[96] THE GUARDIAN. *Lithuania tells citizens to throw out Chinese phones over censorship concerns.* [online]. 2021. [cit.2022-01-30]. Dostupné z: https://www.theguardian.com/world/2021/sep/22/lithuania-tells-citizens-to-throw-out-chinese-phones-over-censorship-concerns

[97] CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM. *Všechno, co jste kdy chtěli vědět o strategické komunikaci (ale báli jste se zeptat).* MVČR. [online]. 2021. [cit. 2022-01-31]. Dostupné z: https://www.mvcr.cz/cthh/clanek/vsechno-co-jste-kdy-chteli-vedet-o-strategicke-komunikaci-ale-bali-jste-se-zeptat.aspx

institucemi k propagaci činnosti úřadů na denní bázi, nikoliv jen k prezentování dosažených úspěchů. Zlidštění státní správy může přinést kýženou důvěru obyvatelstva a předejít následnému šíření dezinformací.

V České republice operují dezinformátoři především na svých webových stránkách (Sputnik CZ, AC 24, Parlamentní listy) a sociálních sítích. I když jejich oficiální stránky na Facebooku nemají velký počet sledujících, jejich zprávy plné dezinformací se snadno dostávají do podvědomí lidí. Veřejné instituce (AV ČR, Česká lékařská komora, apod.) se snaží od takovýchto dezinformačních zpráv distancovat a vyvracet je. Přesto nejsou vyvráceny díky nejednotnosti předních českých osob. Do budoucna je tedy třeba sjednotit názory čelních představitelů státu (vědců) a cíleně dementovat signifikantní dezinformace, které ohrožují zájmy ČR. Česká legislativa také musí projít zásadními změnami, aby mohly mít bezpečnostní složky možnost kontroly sdíleného obsahu na internetu. Během pandemie byl internet zahlcen poplašnými zprávami a dezinformacemi, například na téma COVID-19. Jediný účinný postup proti šíření těchto zpráv jsou tvrdé sankce vůči jejich původcům. V případě šíření neověřených zpráv je nutné stejně tvrdě postupovat i vůči webovým platformám Musí být vytvořen účinný mechanismus kontroly, který zabrání dezinformační kampani cizích mocností na území ČR.

7.3 Diplomacie a spolupráce v mezinárodních společenstvích

Pro Pobaltí i Českou republiku je velmi důležité členství v mezinárodních organizacích. Úkolem NATO je ochrana svobody a zajištění bezpečnosti členů pomocí politických a vojenských prostředků. Společným úsilím lze předejít konfliktům a budoucím problémům. V rámci krize může NATO povolat vojenskou obranu do jednotlivých států. Přítomnost eFP v Pobaltí zaručuje preventivní způsob předcházení budoucího konfliktu, který by mohl nastat s Ruskou federací. Je nutné, aby zde tyto jednotky byly přítomny a působily jako odstrašení. Baltské státy přispívají 2 % do rozpočtu NATO a zaručují, že budou jednat v jeho zájmu. Lotyšsko a Estonsko se podílí na dvou významných projektech, a to na CCDCOE a StatCom COE. Jejich cílem je vytváření obranných kybernetických strategií, včetně komunikace. Díky rozmachu hybridních hrozeb je nutné, aby se do těchto projektů zapojilo co nejvíce států a napomáhaly jejich rozvoji. Česká republika

musí splnit závazek 2 % HDP do rozpočtu NATO. Její prioritou by mělo také být podílení se na rozvoji a posilování vlivu v NATO.

Vstup do Evropské unie zajistil Estonsku, Lotyšsku, Litvě i České republice mnoho benefitů. Díky ní se lépe integrovali se státy západní Evropy a rozvinul se domácí trh i mezinárodní obchod. Malé státy potřebují mezinárodní společenství, která budou podporovat jejich integritu a integraci. Do budoucna je třeba, aby EU i NATO byli jednotnými silnými společenstvími, které zajistí rozvoj a ochranu zájmů svých členských států.

7.4 Ozbrojené složky a obrana

Česká republika a Estonsko s Lotyšskem mají poměrně malé armády. Je třeba doplnit jejich počty, aby odpovídaly současným potřebám. ČR musí adekvátně podporovat svou armádu a navýšit její rozpočet, zajistit obnovu výzbroje a pravidelný výcvik a skutečně se řídit cíli, které jsou vytyčeny v Obranné strategii ČR z roku 2017 a v Dlouhodobém výhledu pro obranu. Ve státech Pobaltí civilní složky aktivně spolupracují s těmi vojenskými. Česká republika musí zaručit, aby se také naše vojenské jednotky účastnili cvičení společně s civilisty. Zároveň je třeba vytvořit nový státní krizový plán, který praktikují a aktivně nacvičují Baltské státy. Celosvětová pandemie ukázala, že Česká republika není připravena na krize. Nová krizová strategie musí zahrnovat spolupráci všech článků státu. Strategie musí nabízet řešení pro potencionální válečné, hybridní, ekonomické nebo pandemické krize. Samozřejmostí je tento plán každoročně procvičovat a aktualizovat. Je nutné usilovat o implementaci nových průlomových technologií v obraně, především kybernetiky a umělé inteligence. Celý systém musí být provázán na mezinárodní společenství, například na lokální V4 nebo NATO. Státy musí sdílet nejlepší zkušenosti z praxe, aby předešly nečekaným hybridním útokům.

Konvenčními hrozbami jsou i nadále ruská vojska, která jsou strategicky rozmístěná na hranicích s Pobaltím. Nesmí být opomenuta ani jejich prezence na Ukrajině a riziko vzniku nové války. Armády společně s NATO musí být připraveny koordinovaně čelit potenciálnímu útoku.

7.5 Energetika

Hybridní hrozby vůči ČR i Pobaltí spočívají také v zástavě dodávek strategických surovin ze zahraničí, jako je ropa nebo zemní plyn. Díky historické provázanosti Východního bloku jsou strategické suroviny stále dováženy především z Ruska. Od vstupu do EU se Pobaltí alespoň částečně oprostilo od absolutní závislosti na monopolních dodávkách některých zdrojů energie. Estonsko je spojeno podmořským kabelem vysokého napětí s Finskem a Litva s Polskem a Švédskem. Vznikly také nové plynárenské projekty. Mezi Litvou a Polskem je stavěn plynovod *GIPL*, který má být uveden do provozu během roku 2022. Po dokončení je jeho cílem propojit Pobaltí a Finsko na jednotnou plynárenskou přepravní soustavu EU. Dalším je *Baltic Connector*, plynovod propojující Estonsko s Finskem[98]. Do budoucna je nutné tyto projekty dále rozvíjet, aby se diverzifikoval prostor s energetickými dodavateli. Je nutné zajistit regionální energetickou politiku a spolupráci. Pobaltí má nedostatečně zabezpečenou ochranu kritické energetické infrastruktury, do budoucna musí vytyčit společný krizový plán.

Energetická závislost České republiky je především na dodávkách ropy a zemního plynu, které zajišťují ropovody *Ingolstadt* z Německa a *Družba* z Ruska. Plynovody jsou napojeny na *Nord Stream 1.* Je nutné, aby ČR investovala do obnovitelných zdrojů a alternativních pohonů, aby se stala více soběstačnou. Zároveň musí prověřovat důležité investory podílející se na energetice, zejména zvolit adekvátní společnost k dostavbě jaderné elektrárny v Dukovanech. Stejně jako Pobaltí musí ČR aktualizovat a vytyčit energetický krizový plán.

Pobaltí i ČR také musí zajistit dostatečné množství hmotných rezerv pro případ výpadku dodávek strategických surovin a energií.

7.6 Finance

Veřejné finance vynaložené na zabezpečení státu jsou téměř ve všech zmíněných zemích neadekvátní. Bezpečnost států je přímo závislá na jejich schopnostech hospodařit a všechny deficity rozpočtů je přímo ohrožují. Podhodnocení rozpočtů

[98] PONARS EURASIA. *The Baltic States and Energy Security.* Univesity of Bologna. [online]. 2020. [cit. 2022-01-29]. 5 s. Dostupné z: https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm665_Riva_July2020_0.pdf

armád nebo nedostatečné financování digitalizace veřejné správy jsou obrovskými překážkami pro budoucí stabilitu zemí. Je nutné masivně investovat do zabezpečení kritické infastruktury, včetně již zmíněné modernizace armády a IT. Česká republika může využít příklad Estonska, které ročně investuje 1 % HDP do digitalizace a díky tomu ušetří další 2 % HDP. Prioritou je dále pro Českou republiku zajistit rozpočet, který bude dlouhodobě snižovat státní dluh díky rozumným investicím do rozvoje země. Zároveň je třeba, aby země transparentně prověřovaly zahraniční zakázky v případě krátkodobých i dlouhodobých investic.

7.7 Zpravodajské služby

Zpravodajské služby zajišťují aktivní ochranu před hybridním působením v jednotlivých státech. Ochraňují demokracii, státní suverenitu a územní celistvost. V případě podezření na kontrarozvědnou činnost informují své nejvyšší představitele a podnikají kroky, aby byla zachována stabilita státu. Rozvědná činnost také spočívá ve spolupráci se zahraničními zpravodajskými službami. Chrání také tajemství NATO a EU a řídí se dokumenty *Strategie pro úlohu NATO v boji proti hybridnímu válčení* a *Společný rámec pro boj proti hybridním hrozbám: Reakce EU*. Je ustanovená také společná zpravodajská bezpečnostní divize, která analyzuje hybridní působení v aliančních státech. Společnými silami varují před nenadálými skrytými hrozbami. Pro svou činnost využívají, především vojenské rozvědné služby, všechny zpravodajské větve HUMINT, SIGING, IMINT i OSINT. Každý rok vydávají zprávy o svých zjištěních, díky tomuto zajišťují informovanost veřejnosti. Je nutné, aby se výsledky zpravodajských služeb řídili nejvyšší zástupci všech států. Jestliže v některých státech dochází k podlamování důvěry v demokratické zřízení působením zahraničních špionů a dezinformátorů, je naprostou prioritou, aby o tom zpravodajské služby informovaly nejvyšší představitele státu a situace byla co nejdříve vyřešena. Příkladem budiž odhalení zahraniční zpravodajské sítě na ruské ambasádě v Praze a běloruské v Litvě.

7.8 Veřejný pořádek a právní stát

Estonsko, Lotyšsko, Litva i Česká republika jsou svrchovanými, jednotnými demokratickými právními státy. Jejich základem je úcta k právům a svobodám člověka a občanů. Státy musí zajišťovat jednotu a propojenost jejich základních

institucí. V rámci kooperace jednotlivých složek je nutné vytvářet a řídit se vytyčenými strategiemi, případě krizovými plány. Při krizi je třeba aktivizace národních bezpečnostních rad, které koordinují bezpečnostní chod států. Tyto bezpečnostní národní rady musí také spolupracovat s regionálními radami na úrovni krajů. Cílem je zlepšit a zajistit strategickou komunikaci s veřejností. Právě veřejnost by se měla podílet na vytváření bezpečného prostředí ve státu. Lotyšsko využívá národních summitů, kde se prezentují názory a praktiky veřejnosti co se bezpečnostní oblasti týče a hlavní instituce přebírají některé jejich poznatky k vytváření strategických plánů.

Ve všech státech je nutné zajistit spolupráci veřejného sektoru, soukromého sektoru a akademické sféry, protože se hybridní hrozby týkají celé společnosti. Představitelé akademické sféry by se měli podílet na celkovém zlepšení bezpečnostní situace, měly by vytvářet studie a analýzy hrozeb. Tyto instituce musí být v úzké spolupráci se svými vládami. Zároveň se na tomto musí podílet i soukromé společnosti, které mají své prostředky na rozvoj zabezpečení interních dat. Parlamenty jednotlivých zemí se musí zabývat podněty od soukromé a akademické sféry k vytvoření nové legislativy. Ta by se měla zabývat současnými typy hrozeb, zejména kybernetickým zločinem. Organizovaná kriminalita, která je pro kybernetický zločin typická, přesahuje národní hranice. Proto je třeba, aby jednotlivé státy spolupracovaly a vytvořily společnou legislativu upravující tyto aspekty.

Závěr

Cílem této bakalářské práce bylo vymezení pojmu hybridní hrozby a následná komparace bezpečnostní agendy jednotlivých Baltských států a České republiky.

Hybridní hrozby jsou realizovány pomocí konvenčních i nekonvenčních prostředků koordinovaných v rámci různých forem informační války, finanční války, sabotáží či kybernetických útoků. Rychlost a rozsah těchto praktik se díky stále dokonalejším a výkonnějším technologiím zvětšuje. Technologie se stále vylepšují a s nimi se vylepšují i metody hybridního působení. Především digitální systémy a jejich snadná dostupnost zvyšují riziko zneužití osobních informací uchovaných v kybernetickém prostoru. Terčem hybridních hrozeb jsou všichni, jejichž zájmy jsou předmětem útočníků. Lze jim čelit jen díky komplexní celospolečenské spolupráci. Je třeba vzdělávat a školit státní aparát i obyvatelstvo ohledně digitální hygieny, zajistit bezplatné kurzy internetové gramotnosti. Je také důležité, aby si občané uměli ověřovat informace, které přebírají z internetových zdrojů. Informační technologie, vysoký počet uživatelů internetu, chytré algoritmy a zejména sociální sítě umožňují rychlé šíření dezinformací. Česká republika i Pobaltí čelí rozsáhlé dezinformační kampani ze strany Ruské federace. Jeho cílem je především podrývání demokratických principů a ovlivňování zahraničního obyvatelstva ruským narativem událostí. Využívá dezinformační média, především proruské weby a ruské televizní stanice vysílající i v Baltském regionu. Je nutné zajistit efektivní obranu proti šíření těchto dezinformací v podobě sankciování jejich šiřitelů a jednotnému vyvracení jejich tvrzení. Státy se do budoucna musí v rámci mezinárodního společenství podílet na rozvoji efektivního systému k předcházení těmto dezinformacím. Zároveň by měly využít cílené strategické komunikace ze strany státních institucí.

Česká republika, Estonsko, Lotyšsko i Litva jsou malými státy, které potřebují mezinárodní společenství. Je nutné spolupracovat s lokálními i světovými organizacemi, které budou upevňovat státní integritu a společnou obranu. Všechny státy se musí aktivně podílet na rozvoji principů společné obrany a posilovat vliv mezinárodních uskupení na státy třetích stran. Musí se účastnit v institucích NATO a posilovat důvěru občanů v jeho funkci.

Česká republika se musí adaptovat a plnohodnotně využít všech možností 21. století. Musí digitalizovat, a to nejen zmiňovanou státní správu a zabezpečit existenci obranných systémů. Může využít nejlepších zkušeností z Pobaltí, především z Estonska a Lotyšska.

Všechny státy musí navýšit počty vojáků do svých armád, případně zavést obdobu povinné vojenské služby. Příkladem můžou být například týdenní krizová cvičení, která každý rok musí být absolvována každým občanem mezi 18 a 59 lety. Česká republika musí také masivně investovat do modernizace vybavení, které v současné době neodpovídá potřebám současnosti. Dále musí inovovat IT systémy a jejich zabezpečení. V neposlední řadě je nezbytné zajistit efektivní cvičení ve spolupráci s civilními složkami (IZS) po vzoru Estonska, Lotyšska i Litvy. Společnost musí důvěřovat článkům zajišťující bezpečnost státu. Jednotlivé státy by se také měli podílet na zvyšování kredibility těchto institucí mezi občany.

Jedním z nejdůležitějších bodů této práce je také aktivní spolupráce mezinárodních institucí se státy, včetně veřejného, soukromého i akademického sektoru. Společnost může být odolná jen za předpokladu, že bude jednotná. Nelze rozdělovat, mezinárodní organizace, státy i sami lidé musí usilovat o soudržnost. Hybridní kampani nelze čelit samostatně. Je třeba zajistit spolupráci všech složek společnosti. Lidé musí být připraveni na budoucí nevyzpytatelné situace, a musí se řídit heslem *expect unexpected,* tedy očekávat neočekávatelné. Pojem válka a mír se v dnešní době stírají, nejsou ohraničené, stejně jako nejsou ohraničené ani hybridní hrozby. Nikdo neví, kdo bude jejich cílem, jakým způsobem, a především – kdy zaútočí. Zasahují všechny, bez výjimky.

Seznam použité literatury

Monografie

ALVAROVÁ, Alexandra. *Průmysl lži: propaganda, konspirace a dezinformační válka.* 2., rozšířené vydání. Praha: Stanislav Juhaňák – Triton, 2019. 308 stran. ISBN 978-80-7553-682-2.

ARMÁDA ČR. *Obranná strategie České republiky.* Praha. [online]. 2017. [cit. 2022-01-20]. 16 s. ISBN 978-80-7278-702-9. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/Obrann___strategie_2017_-_CZ.pdf. s.11-13.

A.RADIN. *Hybrid Warfare in the Baltics: Threats and Potentional Responses*. RAND Corp. Santa Monica, California. [online]. 2017. [cit. 2021-11-16]. 58 s. ISBN 13 978-0-8330-9558-9. Dostupné z: apps.dtic.mil/sti/pdfs/AD1085287.pdf. s.18.

DANICS Š., STRNAD Š. . *Aspekty bezpečnosti*. PAČR. 2016. 136 s. ISBN 978-80-7251-455-7. S.7, 58

GEDAYOVÁ, M. *Srovnávací studie: Komplexní přístup Severoatlantické aliance a Evropské unie při řešení krizí.* Ochrana & Bezpečnost. Praha. [online]. 2015. [cit. 2021-08-05]. ISSN 1805-5656. 63 s. Dostupné z: http://ochab.ezin.cz/O-a-B_2015_A/2015_A_09_gedayova.pdf, s.1-2

Gen. CONWAY. A Cooperative Strategy For Maritime Security. Washington. [online]. 2007. [cit. 2021-08-05]. 20 s. Dostupné z: https://www.uscg.mil/Portals/0/Strategy/MaritimeStrategy.pdf

HOFFMAN, F. G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute, USA. [online]. 2007 [cit. 2021-07-16]. 72 s. Dostupné z: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

JAGELLO 2000. *Hybrid warfare: A new phenomenon in Europe's security environment. Updated and extended 2nd edition*. Praha: Jagello 2000 for NATO Information Centre in Prague, 2016. 29 s. ISBN 978-80-904850-5-1.

KOOK L. *Estonian Discourse on Cyber Risk and Security Strategy*. University of Tartu and University College London. Tallinn. 2018. [cit. 2021-11-12]. 72 s. Dostupné z: digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1136&context=scholcom. S. 45-47

LASCONJARIAS G., LARSEN J.A. *NATOs response to hybrid threats*. Debooks Italia, 2015. 372 s. ISBN 978-88-96898-12-3. Dostupné z: https://www.files.ethz.ch/isn/195405/fp_24.pdf

McCULLOH TIMOTHY B. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* Kansas. [online]. 2012. [cit. 2022-07-16]. 61 s. Dostupné z: https://www.hsdl.org/?view&did=758318. s.IX

POKORNÝ L.; CHROBÁK J.; FLIEGEL M. *Zákon o zpravodajských službách České republiky. Zákon o Bezpečnostní informační službě. Zákon o vojenském zpravodajství. Komentář.* Praha: Wolters Kluwert. ČR. 2018. ISBN 978-80-7552-378-5. 204 s.

PONARS EURASIA. *The Baltic States and Energy Security.* Univesity of Bologna. [online]. 2020. [cit. 2022-01-29]. 5 s. Dostupné z: https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm665_Riva_July2020_0.pdf

TÁBORSKÝ, Jiří. *V síti (dez)informací: proč věříme alternativním faktům*. První vydání. Praha: Grada Publishing, 2020. 224 stran. ISBN 978-80-271-2014-7. Dostupné také z: https://www.bookport.cz/kniha/v-siti-dezinformaci-6094.

Časopisecké články

BAHENSKÝ, V. *PARADOX OF HYBRID WAR: On Causes and Implications of Pragmatism in the Debate.* Obrana a strategie. [online]. 2018. 12 s. [cit. 2021-07-16]. ISSN 12146463. Dostupné z: doi:10.3849/1802-7199.18.2018.02.089-100. s. 89-100

STOJAR, R. *Vývoj a proměna konceptu hybridní války*. Vojenské rozhledy. 2017. [cit. 2021-07-16]. ISSN 1210-3292, 2336-2995. 12 s. Dostupné z:

https://vojenskerozhledy.cz/kategorie-clanku/ozbrojene-konflikty/vyvoj-a-promena-konceptu-hybridni-valky

Konferenční příspěvky

A. KOZLOWSKI. *Comparative Analysis Of Cyberattacks On Estonia, Georgia And Kyrgyzstan.* University of Lodz, PL. 2013. [cit. 2021-11-12]. 10 s. Dostupné z: https://www.researchgate.net/profile/Nnedinma-Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000/International-Scientific-Forum-ISF-2013vol3.pdf#page=246. s. 237-238

FRASZKA B. *Baltic States versus Russian Hybrid Threats.* Warsaw Institute. [online]. 2020. [cit. 2022-01-30]. 16 s. Dostupné z: https://warsawinstitute.org/wp-content/uploads/2020/10/BALTIC-STATES-VERSUS-RUSSIAN-HYBRID-THREATS-Bartosz-Fraszka.pdf, s.10

KOPEČNÝ T., VRÁBEL F., STŘEDULA J., arm. gen. PAVEL P. . Panel 3 / Výzvy: *Bezpečnost v éře dezinformací, šedá zóna jako nová doména a systém protikrizové ochrany: co hrozí a co zmůžeme?* Konference Naše bezpečnost není samozřejmost. [online]. 22. 6. 2021. [cit. 2021-08-09]. Dostupné z: https://www.nbns.cz/2021-program-konference

Zákony a dokumenty států a mezinárodních institucí

AIZSARDZĪBAS MINISTRIJA. *Comprehensive National Defence in Latvia*. [online]. 2020. [cit. 2022-01-23]. 7 s. Dostupné z: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mod.gov.lv%2Fsites%2Fmod%2Ffiles%2Fdocument%2FComprehensive%2520National%2520Defence%2520in%2520Latvia.docx&wdOrigin=BROWSELINK

AIZSARDZĪBAS MINISTRIJA. *The National Security Concept*. Latvia. [online]. 2020. [cit. 2022-01-23]. 29 s. Dostupné z: https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf

BALTIC ASSEMBLY. *RESOLUTION of the 40th Session of the Baltic Assembly*. Vilnius, Litva. [online]. 2021. [cit. 2022-01-14]. 9 s. Dostupné z https://www.baltasam.org/uploads/article-files/files/2_Resol_2021_ENGL.pdf. s.6

CROSS-SECTORAL COORDINATION CENTER. *National Development Plan of Latvia for 2021-2027.* Riga. [online]. 2020. [cit. 2022-01-23]. 89 s. Dostupné z: https://www.pkc.gov.lv/sites/default/files/inline-files/NAP2027__ENG.pdf

ESTONIAN MINISTRY OF DEFENCE. *National Defence Strategy*. Estonia. [online]. 2011. [cit. 2021-11-12]. 28 s. Dostupné z: https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf . s.10

EUROPEAN COMMISION. *Digital Government Factsheet 2019 Latvia*. Latvia. [online]. 2019. [cit. 2022-01-23]. 45 s. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Latvia_2019.pdf . s. 6

GOVERNMENT OF THE REPUBLIC OF LITHUANIA. *National Cyber Security Strategy.* Lithuania. [online]. 2018. [cit. 2022-01-25]. 20 s. Dostupné z: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

MINISTERSTVO OBRANY ČR. *Audit národní bezpečnosti*. [online] 2016. [cit. 2021-08-09]. 142 s. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf. s. 27-38, 51,52-61

MINISTERSTVO OBRANY ČR. *Dlouhodobý výhled pro obranu 2035.* Praha. [online]. 2019. [cit. 2021-10-13]. 36 s. Dostupné z: https://www.mocr.army.cz/images/id_40001_50000/46088/2035.pdf

MINISTERSTVO OBRANY ČR. *Národní strategie pro čelení hybridnímu působení*. Praha. [online]. 2021. [cit. 2021-09-20]. 12 s. Dostupné z: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

MINISTERSTVO OBRANY ČR. *Obranná strategie České republiky.* Praha. [online]. 2017. [cit. 2021-10-13]. ISBN 978-80-7278-702-9. 16 s. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/Obrann___strategie_2017_-_CZ.pdf

MINISTERSTVO VNITRA ČR, odbor bezpečnostní politiky. *Zpráva o extremismu a předsudečné nenávisti na území České republiky v roce 2020.* [online] Praha. 2021. [cit. 2021-09-20]. 31 s. Dostupné z: https://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. Praha. [online]. 2015. [cit. 2021-08-07]. ISBN 978-80-7441-005-5. 24 s. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

MINISTRY OF DEFENCE. *CDU Concept*. Latvia. [online]. 2013. [cit. 2022-01-23]. 8 s. Dostupné z: https://www.mod.gov.lv/sites/mod/files/document/cyberzs_April_2013_EN_final.pdf

NB8. *NB8 WISE MAN REPORT*. Riga, Kodaň. [online]. 2010. [cit 2022-01-14]. 28 s. Dostupné z: https://vm.ee/sites/default/files/content-editors/NB8WiseMenReport.pdf?_x_tr_sl=auto&_x_tr_tl=cs&_x_tr_hl=en-US&_x_tr_pto=wapp

NÚKIB. *DoS/ DDoS útoky*. GovCERT. Praha. [cit. 2021-11-12]. 4 s. Dostupné z: https://nukib.cz/download/publikace/doporuceni/Doporuceni_DDoS.pdf

NÚKIB. *Národní strategie Kybernetické bezpečnosti České republiky* In: Praha. [online]. 2020. [cit. 2021-10-13]. 24 s. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

REPUBLIC OF ESTONIA: MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS. *Cybersecurity Strategy 2019-2022*. [online]. 2019. [cit. 2022-01-23]. 71 s. Dostupné z: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

REPUBLIC OF ESTONIA: MINISTRY OF FOREIGN AFFAIRS. *Estonian Foreign Policy Strategy 2030*. Tallinn. [online]. 2020. [cit. 2022-01-23]. 42 s. Dostupné z: https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/estonian_foreign_policy

_strategy_2030_final.pdf#:~:text=The%20Foreign%20Policy%20Strategy%20has%20been%20drawn%20up,of%20Estonia%E2%80%99s%20inter-%20ests%20in%20a%20changing%20environment

REPUBLIC OF LITHUANIA. *Law on the Basics of National Security*. [online]. 1997. [cit. 2022-01-20]. 25 CH. Dostupné z: https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=9tq147ume&documentId=TAIS.39790&category=TAD. H16

RIIGIKOGU. *National Security Concept 2017*. Estonia. [online]. 2017. [cit. 2022-01-21]. 22 s. Dostupné z: https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf

SEIMAS OF THE REPUBLIC OF LITHUANIA. *National Security Strategy*. Lituhania. [online]. 2017. [cit. 2022-01-21]. ISBN 978-609-412-113-5. 20 s. Dostupné z: https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf

STATE SECURITY DEPARTMENT OF THE LITHUANIA AND DEFENCE INTELLIGENCE AND SECURITY SERVICE UNDER THE MINISTRY OF NATIONAL DEFENCE. *National Threat Assessment 2021.* Lithuania. [online]. 2021. [cit. 2022-01-03]. 78 s. ISSN 2669-2732. Dostupné z: https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf . s. 15, 18-23, 41-43, 46-47

VLÁDA ČR. *Statut Bezpečnostní rady státu*. Příloha č. 1 k usnesení vlády ze dne 9. července 2014 č. 544 ve znění usnesení vlády ze dne 10. května 2017 č. 360, usnesení vlády ze dne 18. dubna 2018 č. 247, usnesení vlády ze dne 10. července 2018 č. 457 a usnesení vlády ze dne 24. října 2018 č. 692 .[online]. 2018. [cit. 2021-10-04]. 5 s. Dostupné z https://www.vlada.cz/assets/ppov/brs/Statut-BRS-rijen-2018.pdf

Webové zdroje a články

ADAMI M. *Lithuania expels two Belarusian diplomats*. Politico. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.politico.eu/article/lithuania-expels-two-belarusian-diplomats/

A.TSATUROV. *Implications for NATO: Latvia and the Russian Hybrid Warfare Threat*. The International Affairs Review. [online]. 2020. Dostupné z: https://www.iar-gwu.org/print-archive/implications-for-nato-latvia-and-the-russian-hybrid-warfare-threat . s.61

ALLIED LAND COMMAND NATO. *EFP*. NATO. [online]. 2022. [cit. 2022-01-22]. Dostupné z: https://lc.nato.int/operations/enhanced-forward-presence-efp

CCDCOE. *About Us.* NATO. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://ccdcoe.org/about-us/

CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM. *Všechno, co jste kdy chtěli vědět o strategické komunikaci (ale báli jste se zeptat).* MVČR. [online]. 2021. [cit. 2022-01-31]. Dostupné z: https://www.mvcr.cz/cthh/clanek/vsechno-co-jste-kdy-chteli-vedet-o-strategicke-komunikaci-ale-bali-jste-se-zeptat.aspx

CERT.LV. *About Us*. Latvia. [online]. 2022. [cit. 23.01.2022]. Dostupné z: https://cert.lv/en/about-us

CSIRT.cz. *O týmu CSIRT.cz*. ČR. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://csirt.cz/cs/o-nas/

ČEŠTÍ ELFOVÉ. *Analýza: Překryv Parlamentních listů a ruského Sputniku.* [online]. 2021. [cit. 2022-01-29]. Dostupné z: https://cesti-elfove.cz/analyza-prekryv-parlamentnich-listu-a-ruskeho-sputniku/

E-ESTONIA*. i-Voting.* Estonia. [online]. 2021. [cit. 2021-11-15]. Dostupné z: https://e-estonia.com/solutions/e-governance/i-voting

E-ESTONIA. *We have built a digital society and we can show you how*. Estonia. [online]. 2021. [cit. 2021-11-15]. Dostupné z: https://e-estonia.com/

ESTONIAN POLICE AND BORDER GUARD BOARD. *The Story and Values*. Estonia. [online]. 2021. [cit. 2021-11-12]. Dostupné z: https://www.politsei.ee/en/the-story-and-values

HERSZENHORN D.M. . *Belarus expels Lithuanian diplomats as ties with EU crumble.* Politico. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.politico.eu/article/belarus-expels-diplomats-as-ties-with-eu-crumble/

ICDS. *About ICDS*. Estonia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://icds.ee/en/about/

KAITSEPOLITSEIAMET. *General Information*. Estonsko. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://kapo.ee/en/content/general-information-0/

LITHUANIAN ARMED FORCE. *Who are we?* Lithuania. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.kariuomene.lt/en/who-we-are/military-service/23649

LRT. *Secrecy'at Belarus nuclear plant a danger to Lithuania – intelligence.* Lithuania. [online]. 2021. [cit. 2022-02-02]. Dostupné z: https://www.lrt.lt/en/news-in-english/19/1358172/secrecy-at-belarus-nuclear-plant-a-danger-to-lithuania-intelligence

M.CESARE. *Russian Encroachment in the Baltics: The Role of Russian Media and Military.* Foreign Policy Research Institute. [online]. 2020. [cit. 2021-11-16]. Dostupné z: https://www.fpri.org/article/2020/12/russian-encroachment-in-the-baltics-the-role-of-russian-media-and-military-2/

MILITĀRĀS IZLŪKOŠANAS UN DROŠĪBAS DIENESTS. *About Us*. Latvia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://midd.gov.lv/en/about-us

MINISTRY OF THE INTERIOR. *Latvian counter-terrorism strategy developed by the State Security Service approved*. [online]. 2021. [cit. 2022-01-24]. Dostupné z: https://www.iem.gov.lv/en/article/latvian-counter-terrorism-strategy-developed-state-security-service-approved

MV ČR. *Co jsou hybridní hrozby.* Centrum proti terorismu a hybridním hrozbám [online]. 2021. [cit. 2021-10-04]. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

NATO STRATCOM COE. *About NATO StratCom COE*. Riga. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

NATO. *NATO's Enhanced Forward Presence*. [online]. 2019. [cit. 2022-01-22]. Dostupné z: https://www.mfa.gov.lv/en/media/2228/download

NBÚ. *O nás – NBÚ*. Praha. [online]. 2021. [cit. 2022-10-04]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/#otazka01

NSCS. *About Us*. Lithuania. [online]. 2022. [cit. 2022-01-23]. Dostupné z: https://www.nksc.lt/en/structure.html

NÚKIB. *NÚKIB*. Praha. [online]. 2021. [cit. 2021-10-04]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

OFFICIAL STATISTICS PORTAL. *Access of Internet by households*. Latvia. [online]. 2022, [cit. 2022-01-23]. Dostupné z: https://stat.gov.lv/en/statistics-themes/information-technologies/computers-and-internet/5675-access-internet-households?themeCode=DL

PARLIAMENT OF ESTONIA. *The National Defence Committee*. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.riigikogu.ee/en/parliament-of-estonia/committees/national-defence-committee/introduction/

REPUBLIC OF ESTONIA: INFORMATION SYSTEM AUTHORITY. *RFC 2350 Description for CERT-EE*. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.ria.ee/en/cyber-security/cert-ee/rfc-2350.html

SEMANTIC VISIONS. *About us – Semantic Visions*. Praha: Semantic Visions. [online] 2021 [cit. 2021-10-04]. Dostupné z: https://semantic-visions.com/

SIPRI. *Military expenditure by country as percentage of gross domestic product, 1988-2020*. SIPRI. [online]. 2021. [cit. 2021-10-13]. 14 s. Dostupné z: https://sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%E2%80%932020%20as%20a%20share%20of%20GDP%20%28pdf%29.pdf

SIMILAR WEB. *Parlamentní listy.* Similarweb.com. [online]. 2022. [cit. 2022-01-30]. Dostupné z: https://www.similarweb.com/website/parlamentnilisty.cz/#overview

STATE SECURITY DEPARTMENT OF LITHUANIA. I*ntelligence*. Lithuania. [online]. 2020. [cit. 2022-01-21]. Dostupné z: https://www.vsd.lt/en/activities/intelligence/

SUPREME COUNCIL. *About the Police.* Latvia. [online]. 1991. [cit. 2022-01-21]. Dostupné z: https://likumi.lv/doc.php?id=67957

SVOBODA A PŘÍMÁ DEMOKRACIE. *Volební program SPD*. [online]. 2021. [cit. 2021-08-09]. Dostupné z https://www.spd.cz/program-vypis/; VOLNÝ BLOK. *Volební program VOLNÉHO bloku*. [online]. 2021. [cit. 2021-08-09]. Dostupné z https://volnyblok.cz/ostatni/program-volneho-bloku/.

THE CONSTITUTION PROTECTION BUREAU OF THE REPUBLIC OF LATVIA. *Our Task*. Latvia. [online]. 2022. [cit. 2022-01-22]. Dostupné z: https://www.sab.gov.lv/?a=s&id=45

THE GUARDIAN*. Lithuania tells citizens to throw out Chinese phones over censorship concerns.* [online]. 2021. [cit.2022-01-30]. Dostupné z: https://www.theguardian.com/world/2021/sep/22/lithuania-tells-citizens-to-throw-out-chinese-phones-over-censorship-concerns

ÚZSI. *Kdo jsme – ÚZSI*. Praha. [online]. 2021. [cit. 2022-10-04]. Dostupné z: www.uzsi.cz

VALISLUUREAMET. *Estonian Foreign Intelligence Service public report 2021*. Estonia. [online]. 2021. [cit. 2021-11-12]. Dostupné z: https://www.valisluureamet.ee/en.html

VALSTS DROŠĪBAS DIENESTS. *About Us.* Latvia. [online]. 2022. [cit. 2022-01-21]. Dostupné z: https://vdd.gov.lv/en/about/about-us

VALSTS PREZIDENTA KANCELEJA. *National Security Council*. Latvia. [online]. 2021. [cit. 2022-01-23]. Dostupné z: https://www.president.lv/en/national-security-council

VLÁDA ESTONSKA. *Riigikaitseseadus*. Estonia. [online]. 2015. [cit. 2022-01-21]. Dostupné z: https://www.riigiteataja.ee/en/eli/502042019010/consolide