ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

Hybridní hrozby v ČR

Hybrid Threats in the Czech Republic

Bakalářská práce

Studijní program:	Ochrana obyvatelstva
Studijní obor:	Plánování a řízení krizových situací
Autor bakalářské práce:	Zdeněk Kotyk
Vedoucí bakalářské práce:	Ing. Ondrej Pecha

Kladno 2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Kotyk**	Jméno:	**Zdeněk**	Osobní číslo:	**491718**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Plánování a řízení krizových situací**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Hybridní hrozby v ČR

Název bakalářské práce anglicky:

Hybrid Threats In the Czech Republic

Pokyny pro vypracování:

Předmětem bakalářské práce bude zhodnocení schopností bezpečnostního systému ČR čelit ohrožení hybridními hrozbami. V teoretické části práce bude zhodnocena schopnost detekce hybridních hrozeb bezpečnostním systémem ČR (detekce nástrojů ze spektra DIMEFIL). V praktické části práce bude proveden návrh a analýza možných opatření proti hybridnímu působení v jednotlivých doménách. Výsledkem práce bude definování potřebných schopností moderního státu v boji proti hybridním hrozbám.

Seznam doporučené literatury:

[1] Kol. autorů, Národní strategie pro čelení hybridnímu působení: National strategy for coun-tering hybrid interference, Praha: Ministerstvo obrany České republiky - VHÚ Praha, 2021, ISBN 978-80-7278-827-9
[2] KŘÍŽ, Zdeněk, Zdeněk KŘÍŽ, Zinaida SHEVCHUK a Peter ŠTEVKOV, Hybrid warfare: A new phenomenon in Europe's security environment, Praha: Jagello 2000 for NATO Information Centre in Prague, 2015, ISBN 978-80-904850-3-7
[3] ŘEHKA, Karel, Informační válka, Praha: Academia, 2017, ISBN 978-80-200-2770-2
[4] SADIK, Gyray, Europe's Hybrid Threats, Cambridge: Cambridge Scholars Publishing, 2017, ISBN 978-1443881791

Jméno a příjmení vedoucí(ho) bakalářské práce:

Ing. Ondrej Pecha

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2022**
Platnost zadání bakalářské práce: **22.09.2023**

doc. Mgr. Zdeněk Hon, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Hybridní hrozby v ČR vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 12.05.2022 ……..

Zdeněk Kotyk

PODĚKOVÁNÍ

Velmi děkuji vedoucímu své bakalářské práce Ing. Ondrejovi Pechovi za odbornou pomoc, cenné rady, konstruktivní přístup a jeho čas, který mi při zpracování této práce věnoval. Dále děkuji své rodině a svým blízkým za podporu během studia a při psaní této práce. Zvláštní poděkování patří mému nejlepšímu příteli, kolegovi a spolužákovi Josefovi Daniškovi a jeho ženě Kateřině Daniškové za to, že mě motivovali a konstruktivně hodnotili.

ABSTRAKT

Tato bakalářská práce se zabývá zhodnocením schopnosti bezpečnostního systému České republiky čelit ohrožení hybridními hrozbami. Se současným dynamicky se vyvíjejícím prostředím plným nových a stále vylepšujících se technologií narůstá i počet nových a nově se tvářejících hybridních hrozeb. Z důvodu rozsáhlého spektra působnosti jsou tyto hrozby stále více nebezpečné a je těžší zajistit potřebnou ochranu a obranu bezpečnostních zájmů státu a jeho obyvatel proti nim. Ohrožení hybridními hrozbami je v současné době, vzhledem ke snadnému přístupu k moderním technologiím, velmi reálné.

V teoretické části se práce zabývá historii, vývojem a současným stavem války, hybridní války, hybridních hrozeb a stavu bezpečnosti ČR. Charakterizuje subjekty zabývající se činností zajišťující bezpečnost a ochranu státu a jeho obyvatelstva. Práce rozebírá působení hybridních hrozeb v rámci spektra DIMEFIL. Toto spektrum obsahuje sedm domén vlivu: diplomacie/politika, informace, ozbrojené síly, ekonomika, finančnictví, zpravodajství, veřejný pořádek a právní stát. Tyto domény jsou v práci charakterizovány a popsány na příkladu, který souvisí s aktuálním děním na území Ukrajiny. Vlastní kategorii tvoří hrozby v kybernetickém prostředí, kde se sféry vlivu prolínají a činí ofensivní kroky útočníka ještě nebezpečnějšími a více nepředvídatelnými.

V praktické části je provedena analýza pěti vybraných opatření (činnost zpravodajských služeb, informovanost obyvatelstva, kybernetická bezpečnost, mezinárodní smlouvy a dohody, akceschopné ozbrojené síly), která jsou používána k čelení hybridnímu působení napříč sférami vlivu ze spektra DIMEFIL. Následně je u daných opatření vyhodnocena schopnost detekce a čelení hybridním hrozbám. Na základě výsledků práce jsou navrhnuta konkrétní opatření k efektivnější eliminaci hybridních hrozeb a jejich působení.

Klíčová slova

Hybridní válka, hybridní hrozba, Česká republika, bezpečnost, DIMEFIL

ABSTRACT

This bachelor thesis deals with the evaluation of the ability of the security system of the Czech Republic to face the threat of hybrid threats. With the current dynamically evolving environment full of new and ever-improving technologies, the number of new and emerging hybrid threats is growing. Due to the wide range of activities, these threats are increasingly dangerous and it is more difficult to ensure the necessary protection and defence of the security interests of the state and its inhabitants against them. The threat of hybrid threats is currently very real, given the easy access to modern technologies.

The theoretical part deals with the history, development and current state of wars, hybrid wars, hybrid threats and the state of security in the Czech Republic. It characterizes the entities involved in ensuring the security and protection of the state and its population. The work analyses the effect of hybrid threats within the DIMEFIL spectrum. This spectrum contains seven domains of influence: diplomacy/politics, information, the armed forces, economics, finance, intelligence, public order and the rule of law. These domains are characterized and described in an example in connection with current events in Ukraine. The categories themselves form threats in the cyber environment, where spheres of influence intersect and represent the offensive actions of the attacker even more dangerous and unpredictable.

In the practical part, an analysis is made of five selected measures (intelligence activities, public awareness, cyber security, international treaties and agreements, actionable armed forces), which are used to face hybrid action across spheres of influence from the DIMEFIL spectrum. Subsequently, the ability to detect and address hybrid threats is evaluated. Based on the results of the work, specific measures are proposed to more effectively eliminate hybrid threats and their effects.

Keywords

Hybrid war, hybrid threat, Czech Republic, security, DIMEFIL

Obsah

1 ÚVOD

Současný, velmi rapidně se vyvíjející rozmach moderních technologií vytváří celou řadu nově vypadajících hrozeb. Tyto staronového hrozby se díky dnešním vyspělým technologiím rozprostřely do nových sfér vlivu. Z důvodu rozsáhlého spektra působnosti jsou tyto hrozby jednak více nebezpečné a je těžší zajistit potřebnou ochranu a obranu bezpečnostních zájmů státu a jeho obyvatel proti nim.

Hybridní hrozby jsou mixem kombinací ofenzivních činností vedených proti zájmovým subjektům, objektům i jejich nehmotnému vlastnictví v podobě citlivých a důležitých informací a dat.

Ohrožení hybridními hrozbami je v současné době velmi reálné, a to nejen na území České republiky (dále jen ČR), ale i na území, jež jsou součástí partnerských vztahů se členskými státy Evropské unie (dále jen EU) a členskými státy Severoatlantické aliance (dále jen NATO). Ve spolupráci s aliančními partnery se ČR zdokonaluje a připravuje na čelení těmto hrozbám.

Toto téma je v poslední době velmi medializované a probírané. Dost se o něm spekuluje kvůli aktivitě ozbrojených sil Ruské federace (dále jen RF) na území Ukrajiny (dále jen UA). Současně probíhá informační válka, kdy je na jednu stranu ovlivňováno obyvatelstvo RF, kterému tamní média distribuují informace dle potřeb režimu i za pomoci tvrdé cenzury, na druhou stranu jsou tyto informace šířeny pomocí sociálních sítí a dezinformačních medií za hranice RF s cílem, aby tyto dezinformace působili na občany v zahraničí, a to způsobilo názorový nesoulad v postoji ke krizi na UA a přímo tak bylo ovlivňováno veřejné mínění.

Téma jsem si vybral právě z důvodu aktuálnosti, a i díky mému zájmu se lépe orientovat v činnostech souvisejících s hybridním působením. Na první pohled a se základním obecným přehledem v této oblasti je situace hybridních hrozeb docela jasnou záležitostí, ale už pouhým lehčím proniknutím při studiu podkladů do této problematiky jsem doznal, že se nejedná o žádné lehké téma.

Čímž se pro mě stává, ještě zajímavějším. Od práce očekávám rozšíření mých vlastních znalostí a získání přehledu a pojednávaném tématu.

2 CÍLE PRÁCE

Předmětem bakalářské práce bude zhodnocení schopnosti bezpečnostního systému ČR čelit ohrožení hybridními hrozbami. V teoretické části bude zhodnocena schopnost detekce hybridních hrozeb bezpečnostním systémem ČR (detekce nástrojů ze spektra DIMEFIL). V praktické části bude proveden návrh a analýza možných opatření proti hybridnímu působení v jednotlivých doménách. Výsledkem práce bude definování potřebných schopností moderního státu v boji proti hybridním hrozbám.

3 PŘEHLED SOUČASNÉHO STAVU

V posledních několika letech dochází z důvodu globalizace v bezpečnostním prostředí k dynamickým změnám, kdy se objevuje celá řada buď zcela nových, nebo nově zkombinovaných hrozeb, které v minulosti neměli takový význam, jaký jim dává dnešní moderní doba. Z důvodu rozsahu různorodosti, je velmi složité určit nebo odhadnout možné dopady a současně je tudíž velmi obtížné tyto hrozby předvídat. ČR jako členský stát EU a NATO naštěstí není v přímém ohrožení konfrontace vojenskými hrozbami na svém území nebo hranicích se sousedními státy. Jakožto členský stát ČR však sdílí bezpečnostní prostor s partnerskými státy na periferii uvedených mezinárodních organizací, čímž přebírá určitou míru odpovědnosti za obranu a ochranu před reálnými nebo potencionálními hrozbami, kterým musí tyto oblasti čelit. Tyto hrozby zasahují ČR spíše menší intenzitou. Avšak ohrožení hybridními hrozbami je pro naše území velmi současné a reálné.

ČR je v současnosti vystavována hybridnímu působení zejména v oblastech, které jsou ideově a hodnotově zakotveny ve společnosti a v ústavním uspořádání státu. Toto působení se používá zejména k ovlivňování politických struktur a celkového rozhodovacího procesu, soudů, policie, ozbrojených sil, hromadných sdělovacích prostředků a veřejného mínění. Záměrem těchto hybridních aktivit je z pohledu invazivních aktérů narušení stability společnosti a vytvoření prostředí, které je vůči politickému vedení státu nedůvěřivé. Definice hybridních hrozeb jsou nejednotné. Již z doslovného překladu je jasné, že hybridní hrozby vznikají z podstaty věci pomocí kombinací a křížením různých entit (hrozeb). Těmto kombinacím a mixům hrozeb je složitější čelit, protože je těžší rozeznat, zda a o jakou hybridní hrozbu se jedná nebo dokonce, kde má hrozba původ, oproti konvenčnímu stylu vedení války, kde je jasně dané, že jedna strana či spojenectví stran vzájemně působí proti druhé straně nebo jinému spojenectví definovanými prostředky a generickými hrozbami. Tyto hrozby působící v různých doménách spolu navzájem souvisí a většinou pocházejí od jednoho zdroje, který se tímto způsobem snaží dosáhnout určitého cíle. V hybridním působení je komplikovaná tzv. atribuce tj. přisouzení tohoto ohrožujícího působení určitému subjektu.

3.1 Historie hybridních hrozeb, válčení a taktiky

Hybridizace bezpečnostního prostředí probíhá odjakživa, a nenítím pádem ničím zcela novým. Projevuje se například společným působením lidových milic a vojenských jednotek, kooperací mezinárodních bezpečnostních či vojenských aliancí, hybridním působením zpravodajských služeb apod. Postupem času se z důvodu pokroku samozřejmě různě měnily a mění formy, rozsah a dynamika hybridizace.

Hybridní válka je známa téměř od počátku vojenských dějin a provází válčení napříč historií. Již v šestém století našeho letopočtu položil jejích základy geniální stratég, filozof a nadaný generál Sun-c‘, který se rozepisoval o strategiích a vedení války ve svém díle Umění války. Toto mistrovské dílo, je psáno jednoduše, avšak věcně a funkčně. Dodnes patří mezi nejlépe napsaná díla tohoto druhu. Sun-c‘ věděl, že klíčem k rychlému vítězství s minimálními ztrátami a náklady na vedení boje spočívá v pochopení a zmatení nepřítele větším počtem činností než jen přímým útokem. Jeho strategií bylo zajištění co největšího spektra informací, udržování nepřítele v nevědomosti a nejistotě maskováním svých aktivit a s využitím lsti pro uštědření finálního úderu. Tuto metodu o více než osm století později zdokonalili japonští bojovníci „shinobi“. Ti se snažili pomocí atentátů, špionáže a dalších nekonvenčních vojenských metod, udržet svoji nezávislost ve vztahu k sousedním územím, ovládaných samuraji. Svojí vojenskou metodu popsali v knize „Bansenshukai“, čímž si zajistili legendární pověst. Bojovníci „shinobi“ jsou známí jako nindžové a kniha Bansenshukai též jako kniha nindžů nebo umění nindžů. O necelá další čtyři století byla použita metoda nekonvenčního boje ve Válce za nezávislost. Zde američtí patrioti kombinovali partyzánské a informační metody boje, které podporovali ekonomickými blokádami. Díky znalosti místního terénu a prostředí je uměli plně využít ve svůj prospěch. Navíc byli schopní efektivně sbírat informace o svém nepříteli a získat podporu většiny místního obyvatelstva. [1]

> *„Hybridní znamená vzniklý smíšením nebo křížením nějakých entit podle toho, jestli výsledkem je entita složená z původních entit a zachovávající jejich původní vlastnosti nebo zcela nová entita, jejíž vlastnosti mohou být od vlastností původních entit odlišné i zcela nové.“* [2]

Příčiny, které významně ovlivnily historický vývoj hybridizace bezpečnostního prostředí, byly jak bezpečnostní střety, tak i technologický vývoj a jeho implementace v prostředcích hybridního bezpečnostního působení. Průběhem času se bude stále méně stávat hlavním cílem bezpečnostního působení ničení konkrétních zájmových materiálních aktiv a stále více bude cíleno především na účelové ovládnutí chování jejich vlastníků či uživatelů.

Termíny hybridní hrozba, a hybridní válka byly poprvé použity již v 90. letech minulého století v prostředí ozbrojených sil Spojených států amerických (dále jen USA). Hlavním promotérem konceptu hybridní války byl po mnoho let Frank Hoffman, autor jednoho z nejznámějších a nejpoužívanějších pojednání o hybridní válce. Na počátku svého vzniku představoval pojem hybridní válka hlavně pomyslný mix harmonizovaných, souběžně vedených konvenčních a speciálních operací během nestandartních konfliktů. Tento mix měl být uplatňovaný v budoucích konfliktech, které svým charakterem činily k nekonvenčnímu způsobu boje, jako je terorismus, vedení guerillové války, informační války či v nejkrajnějším případě i použití zbraní hromadného ničení.[3]

V roce 2007 se dostal pojem hybridní války a hrozeb do slovníku ozbrojených sil USA a po roce 2010 se tento pojem objevuje i v NATO. V čase se vyvíjející hybridizace bezpečnostního prostředí velmi významně ovlivňuje nejen náplň a průběh bezpečnostních střetů, ale i technologický vývoj a jeho použití v prostředcích hybridního bezpečnostního působení.

3.2 Válka

Válka je otevřený ozbrojený konflikt vyhlášený mezi dvěma stranami. Tyto strany jsou většinou reprezentovány dvěma státy nebo společenskými komunitami. Tento konflikt má za následek přerušení normálních politických a diplomatických aktivit mezi zúčastněnými stranami. Důsledkem konfliktu je mobilizace všech dostupných zdrojů, kterými dané strany disponují. V oblastech, kde ke střetu dochází, může dojít z tohoto důvodu k vyhlášení válečného stavu nebo válečné situace.

Pruský vojenský teoretik a filozof Carl von Clausewitz definoval válku jako *„Pokračování politiky státu násilnými prostředky, které jsou použity k donucení protivníka vykonat naši vůli“.* [4]

3.2.1 **Válečný stav**

Je stav mezi dvěma a více znepřátelenými stranami (státy nebo jinými subjekty mezinárodního práva), který vzniká vypuknutím ozbrojeného konfliktu, a to i bez ohledu, zda byla vypovězena válka. Tuto situace definuje Ústava ČR, jako situaci, kdy je ČR napadena, nebo je-li třeba plnit mezinárodní smluvní závazky o společné obraně (NATO) proti napadení. Válečný stav vyhlašuje dle Ústavního zákona č. 1/1993 Sb., čl. 39, písm. 3 Parlament ČR. [5]

„Válečné umění má pro stát klíčový význam.
Rozhoduje o životě a smrti, o bezpečí, nebo zkáze.
Proto je nutné se jím zabývat a v žádném případě je neopomíjet.“
Sun-c‘ [6, s.8]

Čtyři generace války

Válčení se může rozdělit do čtyř vývojových období nebo spíše generací. První generace byla v období během 17. až do první poloviny 19. století. Vyznačovala se liniovým, řadovým bojem, ve kterém se kladl důraz hlavně na palebnou převahu. Velkou roli zde hrála rychlost palby (přebíjení dle možnosti dostupných zbraní), přesnost a početní převaha.

V druhé polovině 19. století začíná druhé období. Hlavním důvodem byla modernizace výzbroje. Muškety a posléze kulomety již představovali pro liniové a zástupové tvary nepřijatelnou hrozbu a způsobovali nepřípustné ztráty. V druhé generaci, kterou započali Francouzi, se začala využívat centrálně řízená dělostřelecká palba. Tento styl boje byl díky vysoké synchronizaci, kdy se velící důstojníci dostávali do rolí moderních velitelů (ve významu velení a organizování v týlu, mimo hlavní válčící zónu), velmi efektivní. Způsob boje bylo vedení olova na cíl a sami Francouzi prohlašovali, že dělostřelectvo dobývá a pěchota zabírá. Toto období trvalo od druhé poloviny 19. století do začátku první světové války, kdy dělostřelectvo nahradilo letectvo.

Během 20. století probíhalo třetí období, které se vyznačovalo rychlostí manévrů, velkou palebnou převahou a zmiňovanou leteckou podporou. Hlavními průkopníky byli Němci. Strategie třetí generace byla vedena tak, aby byl útok co nejvíce překvapující a rychlý, často vedený do zad nepřítele. Díky tomuto nelineárnímu vedení boje se více zformovala obrana, která musela čelit novému typu boje. Heslem bylo obklíčit a zničit.

Od 90. let 20. století trvá období čtvrté generace. Vyznačuje se velmi nekonvenčním stylem vedení boje, bojiště není zcela specifikováno. V této čtvrté generaci se jako prostředek k dosažení cíle využívá i terorismus či dezinformování, aby bylo co nejrychleji dosaženo žádaného politického nebo vojenského stavu, vyhovujícímu ofenzivnímu aparátu. Je využíváno partyzánských válek a strategií, které by měli vést k vyčerpání státních nebo korporátních zdrojů a sil, a tím tento aparát donutit ke kapitulaci. Velký důraz je kladen na využívání informací a jejich následné ovlivňování, k docílení zamýšleného záměru útočníka. Používá se například k svrhnutí vládnoucí vrstvy nebo místní vlády, někdy i za pomoci místního obyvatelstva, které má protivník díky dezinformacím na své straně. Postupem modernizace a pokroku v digitalizaci sytému a rozvojem médií se pomalu dostáváme do fáze, kdy budou informační a sdělovací média mocnější než obrněná vozidla a zbraně. [7]

3.3 Hybridní válka

Koncept hybridní války je starý jako válka sama, přesto se tento pojem objevuje v odborných kruzích nově. Jak je to možné a co to znamená? Válečný mix, který byl znám již téměř od počátku a vyskytoval se ve velkých historických bitvách, se stal méně obvyklým s mezinárodními smlouvami a novými technologiemi. Hybridní válka vnáší určitou „originalitu“. Tuto originalitu bychom mohly vnímat určitými složitějšími a méně průhlednými konflikty. „Originalita“ současné hybridní války činí pro NATO velmi náročný boj s ní. [8]

Jedná se o ozbrojený konflikt, který kombinuje nevojenské a vojenské prostředky. Cílem tohoto vedení je jejich synergickým efektem přinutit protivníka k učinění takových kroků, které by jinak sám ze strategických důvodů neučinil. Vždy je jedna strana konfliktu zastoupena státem. Hlavní roli při dosažení cílů války hrají

nevojenské prostředky v podobě ekonomických sankcí, embarg, kriminálních aktivit, psychologických operací a propagandy teroristických aktivit a jiných podvratných aktivit obdobného charakteru. Vojenské operace útočníka jsou vedeny skrytě nepravidelnými silami kombinujícími asymetrické a symetrické způsoby vedení bojové činnosti proti celé společnosti. Konkrétními cíli pak jsou zejména její politické struktury, ozbrojené síly, orgány státní správy a samosprávy, ekonomika daného státu a morálka obyvatelstva. [9]

Útočník se namísto složitých vojenských manévrů snaží demoralizovat protivníka. Často do svých aktivit zahrnují použití pestré škály sabotáží, různých dezinformačních kampaní, organizovaných kybernetických útoků a podporují politické nebo separatistické skupin, které jsou ochotné s nimi spolupracovat. Cílem psychologického a politického útoku je rozdělení vojenských a vysoce vzdělaných vrstev společnosti od zbylé průměrné civilní populace. Správné použití takového útoku vede k rozdělení veřejnosti a vytváří tlak na politickou reprezentaci země, která musí obyvatelstvo zase spojit. Koncept vedení hybridní války je zaměřený na válku a mír, a přitom není jasně prokazatelné, kdy válka začíná a kdy končí.

P. Zůna naproti tomu vidí koncept hybridních válek chybný v tom, že nebere do úvahy globální nebo regionální aktéry, kteří mají protichůdné cíle vůči těm našim, ale přesto to neznamená, že neexistuje jiné volby, než sáhnout k legitimnímu násilí v souladu s Chartou Organizace spojených národů (dále jen OSN) nebo rezolucí Rady bezpečnosti OSN. Dalším negativem konceptu je skutečnost, že hlavním záměrem jsou destruktivní způsoby činnosti aktérů, i když jsme každý den svědky toho, že více efektivní důsledky pro úspěšnost koaličních operací mají jiné nástroje, například: informační, politické a samozřejmě ekonomické. [10]

V boji lze použít jen dva druhy útoku, přímý a útok léčkou,
ale jejich kombinací vznikne nepřeberné množství postupů.
Sun-c' [7, s.33]

3.3.1 Charakteristiky a taktiky hybridního vedení boje

- Smíšené taktiky – kombinace vojenských schopností s malými (partyzánskými) jednotkami, asymetrické útoky a mobilní jednotky.
- Flexibilní a adaptibilní taktiky – jelikož jde o jednotky malé, jsou obvykle schopny se transformovat do malé a rychle reagující jednotky nebo do komplexní formace.
- Teroristické a kybernetické útoky.
- Technologicky pokročilé systémy, které jsou schopny být použity nad rámec svého původního určení.
- Propaganda, mediální kontrola, dezinformační kampaň.
- Trestní aktivity jako zdroj peněz nebo útoku, nelegální finanční operace.
- Zaměření se na rozdělení společnosti na více nejednotných, názorově protichůdných skupin. Podrývání její jednoty a eliminace schopnosti uskutečnit obtížná politická rozhodování.
- Nedodržení mezinárodního práva, použití podvratného zpravodajství, sabotáže nebo politická podpora extremistických skupin vyhovujících útočníkovi.
- Finančnictví – různé formy ekonomického nátlaku (uvalení cel, embarg, odepření dodávek surovin nebo energií, destabilizace klíčových odvětví, destabilizace měny, trhu s akciemi a dluhopisy, bankovního sektoru.
- Zpravodajství – aktivity zpravodajských služeb, špionáž, získávání spolupracovníků (zejména státních či politických činitelů) k protistátní činnosti. [11]

Mezi hybridní války zařadil Frank G. Hoffman kromě nejznámějších modelové rusko-čečenské války uskutečněné v letech 1994–1996, také Búrské války, které proběhly v letech 1899–1902, válku v Indočíně konající se v letech 1946–1954, i konflikt v Afghánistánu z let sovětské intervence či konflikt v Libanonu mezi Hizballáhem a Izraelem z roku 2006, kde probíhali partyzánské boje. Jako další konflikt, který podle něj splňuje kritéria vedení hybridní války, F. G. Hoffman uvádí jako téměř „vzorový model hybridního válčení" i „srbský nájezd do Kosova"

uskutečněný v letech 1998–1999, kde se dle jeho mínění spojuje nasazení moderní protivzdušné obrany a obrněné techniky v kombinaci s realizací etnických čistek a „nepravidelnou urbánní taktikou“. [3]

Operace KFOR (Kosovo Force) na Balkáně pod názvem Joint Guardian v Kosovu měla i českou stopu. První kontingent českých vojáků byl tvořen příslušníky prostějovských výsadkářů z 6. průzkumné roty, kteří zde byli nasazeni do ledna 2000, než byli vystřídáni vojáky 4. brigády rychlého nasazení. [12]

> *„Už Československo mělo přímou zkušenost s hybridním válčením, a to například na konci třicátých let minulého století, kdy nacistické Německo zahájilo „hybridní válku“ za pomoci různých nacistických sudetoněmeckých militantních skupin a masivní protičeskoslovenskou propagandou. Situace kulminovala mnichovskou dohodou v září 1938. V roce 1939 pak byla využita kombinace pro-německých a proti-polských postojů k manipulaci v takzvaném Slezském odboji“.* [13]

Čtyři fáze hybridní války

První fáze se snaží o co největší demoralizaci společnosti, za pomoci radikalizace různých skupin obyvatelstva. Snaží se narušit jejich vzájemné vztahy a vnímání problému, k dosažení co nejvíce nestabilního prostředí, ve kterém se může stát záminkou pro konflikt skoro cokoliv. K narušení vztahů se využívá poukázáním na rozpory mezi sociálními podmínkami, v náboženství, v postavení jedinců a jejich moci vlivu či veřejných názoru a sympatií. Mezitím jsou ze strany útočníka podporovány obě strany opačného spektra konfliktů. Tímto jednáním útočník společnost dokonale zatěžuje a postupně ji rozkládá.

V druhé fázi je již společnost na takové úrovni, že se lehce přehlédne další krok útočníka, což je destabilizace současných institucí. Oslabuje zejména strategické instituce ekonomického a právního systému.

Díky tomuto jednání, kdy je společnost demoralizována a instituce destabilizovány nastává třetí fáze. Společnost přestává fungovat a nastává krize. Jedním z důsledku nastalé situace může být vypuknutí občanské války. Společnost

si kvůli aktuálnímu stavu žádá změnu režimu nebo vůdce a očekává zlepšení této situace.

Čtvrtá fáze je následná obnova a návrat do původního stavu nově dosazenými vůdci, kteří často při této obnově eliminují poražené protivníky. [14]

3.4 Hybridní hrozby

Je těžké přesně určit co je a není hybridní hrozbou. Téměř vše je možné nazývat a považovat za hybridní hrozby. Hybridní hrozby jsou fenoménem vyplývajícím z konvergence a propojení různých prvků. Tyto prvky společně tvoří komplexnější a vícerozměrnou hrozbu. Definice, které jsou k hybridním hrozbám dostupné, se velmi blíží definici, kterou je popsána hybridní válka. Autoři zabývající se problematikou konfliktů vedených hybridním způsobem často tyto dva pojmy prolínají a používají dle potřeby.

„Primárně se jedná o metody či způsoby, jakými je vedena konfrontace/konflikt, tj. široká, komplexní, přizpůsobivá a integrovaná kombinace konvenčních a nekonvenčních prostředků, otevřených a skrytých aktivit, majících primárně charakter nátlaku a podvratné činnosti, které jsou prováděny vojenskými, polovojenskými a různými civilními aktéry.“ [15]

V literatuře, bezpečnostních a strategických dokumentech se používá ještě výraz hybridní kampaň či hybridní působení. Spektrum klasických nástrojů, které mohou tvořit součást hybridní kampaně, je označováno zkratkou DIMEFIL. Toto spektrum obsahuje sedm dimenzí moci, které specifikují danou oblast hybridního působení. O spektru DIMEFIL a jeho nástrojích se budeme bavit v samostatné kapitole.

Hybridní působení je skrytá i zjevná činnost státních či nestátních aktérů (původců hybridního působení), která míří proti snadno zranitelným prvkům společnosti a demokratického státu. Původci hybridního působení využívají ve svůj prospěch politické, diplomatické, informační, vojenské, ekonomické, finanční, zpravodajské a další nástroje s cílem narušit chod demokratických institucí, vnitřní

bezpečnost a procesy právního státu. Hybridní působení využívá i legálních a legitimně se jevících nástrojů k dosažení nepřátelských cílů a působí proti zájmům ČR. Rychlost, rozsah a intenzita hybridního působení se v důsledku pokroku a zdokonalováním nových technologií zvyšuje, což činí hybridní hrozby více nebezpečnými. [16]

Hybridní hrozby se do Evropy dostávají v různých formách a působí zejména ze dvou směrů. Jedním směrem jsou nestátní organizace vznikající na Středním a Blízkém východě, které působí jako rozsáhlé nepřátelské buňky napříč kontinenty. Vzhledem k naší geografické poloze je to hrozba z jihu. Hlavním cílem těchto aktérů je vybudovat si co nejsilnější a nejširší struktury vně jiných států a jejich organizací. Tyto struktury mají vést hlavně k získání přístupu k prostředkům sloužícím k vedení boje, které mohou být následně použity k působení násilí na civilizovaném obyvatelstvu Evropy. Druhým směrem je rozsáhlá hybridní kampaň vedena z východu vládou RF. Při této hybridní kampani se RF respektive „prezident Putin“ opírá hlavně o svou mocenskou sílu, kdy hybridní působení vede ve sféře politické (jakožto nejvyšší mocenský aristokrat s podporou všech prostředků státu). Dále díky držení nerostných surovin využívá sféry ekonomické a samozřejmě v neposlední řadě velmi používá sféru informační, a to šířením dezinformací a ovládáním tamních médií. Oba tito aktéři mají na svém poli působnosti určitou centrální kontrolu, kdy mohou koordinovaně využívat všech svých prostředků a nástrojů, což z nich činí potenciální i reálné hrozby. Tyto nepřátelské trendy představují pro ČR potenciální ohrožení. [17]

Terčem hybridních hrozeb jsou jak samostatné subjekty, kterými mohou být jak vlivní lidé (vládní představitelé, církevní hodnostáři, zámožní investoři a promotéři, akademičtí pracovníci apod.) nebo samostatný stát, tak velké organizace (veškeré neziskové organizace, veřejnoprávní média, politické skupiny aj.) i mezinárodní instituce (zejména EU a NATO). Všechny tyto subjekty jsou z hlediska přesvědčení útočníka pro něj nepřátelské, a proto vůči nim vede v rámci hybridního působení různé formy útoku, které považuje v dané sféře za efektivní a potřebné k dosažení vlastních záměrů.

3.4.1 Kybernetické hrozby

Vlastní sférou mezi hybridními hrozbami jsou hrozby kybernetických útoků. V dnešní moderní době se pohybujeme v kyberprostoru pomocí všemožných moderních technologií, které využíváme na denní bázi. Tyto technologie se staly doslova součástí běžného života každého z nás. Rychlá a plošná digitalizace prostředí, ve kterém se nacházíme, dává možnosti pro vytváření nových hrozeb, které jsou specifické pro tento prostor (v kyberprostoru se jednotlivé dimenze moci prolínají). Toto prostředí je již tak dynamické a komplexní, že jeho narušení představuje velmi závažnou bezpečnostní hrozbu. [18]

Nejčastější hrozbou v kyberprostoru bývá exfiltrace dat, pomocí podvodných e-mailů a odkazů. Kompromitací jednotlivých subjektů a vládních institucí získají aktéři nejen informace o postojích a záměrech ČR v určitých tématech, ale rovněž interní informace týkající se konkrétních pracovníků, zaměstnanců či vrcholově postavených členů státu, včetně jejich vlastních názorů a postojů k určitým tématům (např. komentáře a revize u exfiltrovaných dokumentů) či mezilidských vztahů pracovníků (např. z uniklé korespondence). Odcizené informace, které jsou pochopitelně pro danou osobu důležité, pak vzhledem ke svému citlivému obsahu, činí dotyčné osoby zranitelnějšími vůči metodám klasické špionáže. [19]

Díky internetu, sociálním sítím a platformám dochází k abnormálně zrychlenému předávání informací, oproti dřívějšímu způsobu jejich předávání, kdy se tato činnost zajišťovala ústně. Zdlouhavou cestou v delším časovém úseku se ústním předáváním častokrát k posluchačům dostali informace zkreslené a neúplné. Internet a sociální sítě, však předávají informace téměř okamžitě k obrovskému počtu osob ve své původní podobě, kdy jsou tyto informace sdílené a přeposílané v reálném čase. Vzhledem k velkému množství dat a rychlosti šíření, vzniká i více dezinformací, jak cílených, tak vzniklých pouhým tlumočením nebo nepochopením informace v plném kontextu. [20]

3.5 Bezpečnost ČR

Základními pojmy, které se k bezpečnosti pojí, jsou hrozba, riziko a samotný pojem bezpečnost. Hrozba je nezávisle existující a mimo nás stojící činitel. Hrozba

je cokoliv, co má potenciální schopnost, jenž může, ale nemusí poškodit zájmy chráněné státem. Míra velikosti hrozby je dána rozsahem možných škod a časovou osou dopadu. Riziko je všudypřítomné a vyznačuje pravděpodobnost vzniku události, která je pro nás nežádoucí. Riziko vždy můžeme odvodit od konkrétních hrozeb. Míra rizika je proměnlivá v čase a závislá na velikosti dané hrozby. Míra rizika se dá redukovat přijetím efektivních a včasných protiopatření.

„České slovo „bezpečnost“ pochází ze základu „bez péče“ neboli: bez starosti, bez problému, mimo nebezpečí. Pozitivní vymezení je vždy problematické: lze jen obtížně stanovit, od jaké míry je subjekt bezpečný a co vše pro to musí být zajištěno. Podle definice autorů České bezpečnostní terminologie z roku 2002 je rozhodující, zda je subjekt připraven a ochoten se bránit a chránit.“ [21, s.12]

Bezpečnost jako taková je vždy vlastností určitého vztahu. Lze ji charakterizovat jako pojem, který nemá v základu určený konkrétní význam. Můžeme mluvit o bezpečnosti pozitivní a negativní. Negativní bezpečnost bychom mohli rozumět nepřítomnost prostředků potřebných k potlačení rizika, možného nebezpečí a eventuálních hrozeb, které mají negativní vliv na chráněné hodnoty. Pozitivní bezpečnost by byl naopak stav nastolený zajištěním potřebných opatření, které v co největší míře zamezují důsledkům možných rizik a hrozeb. Níže je jedna z definic bezpečnosti pozitivní.

Bezpečnost můžeme definovat jako stav, kdy jsme veškeré možné hrozby eliminovali na co nejnižší možnou míru, která by ohrozila objekty zájmu.

3.5.1 **Bezpečnostní prostředí ČR**

Prostředí, které ovlivňuje ČR, se velmi dynamicky mění. Z důvodů zlepšující se komplexnosti bezpečnostních faktorů a jejich trendů se snižuje předvídatelnost tohoto prostředí. Díky geografickému a geopolitickému postavení ČR v rámci Evropy je pravděpodobnost přímého vojenského ohrožení území ČR a narušení státní svrchovanosti na nízké úrovni. Základem tohoto postavení jsou dobré a vřelé vztahy se sousedními zeměmi a členství v mezinárodních organizacích, zejména v NATO a EU. Avšak hrozbu pro bezpečnost a stabilitu představují nepřátelské akty nacházející se v hraničních částech společného euroatlantického prostoru

a v oblastech s Evropou sousedících. Díky tomuto vlivu nelze zcela vyloučit přímé ohrožení území některých členských zemí NATO a EU, což může mít dopad i na bezpečnost ČR. Díky této provázanosti se vnitřní a vnější bezpečnostní hrozby čím dál více prolínají a rozdíly mezi nimi se pomalu vytrácejí. Ohrožení bezpečnosti spřátelených států a států, jenž jsou členy společných organizací, může mít jak násilnou vojenskou povahu, tak i nespecifikovanou podobu metod takzvaného hybridního válčení. Členstvím v těchto organizacích přebírá ČR určitý díl odpovědnosti za obranu a bezpečnost společného území v systému kolektivní obrany. [22, 23]

Bezpečnost ČR je pevně spjata s bezpečností společného euroatlantického prostoru. Proto se její strategická bezpečnost řídí a vychází i ze základních strategických plánu zanesených v dokumentech NATO a EU.

Hlavní výkonnou mocí, která odpovídá za čelení bezpečnostním a hybridním hrozbám je v ČR vláda, která poté na základě konkrétních hrozeb přijímá potřebná opatření, která by měla zamezit projevům jejich působení. Tato opatření a realizace následných kroků k zamezení projevů těchto hrozeb mají na starosti jednotlivé ústřední státní orgány. Ministerstvo vnitra, Ministerstvo zahraničních věcí, Ministerstvo obrany (dále jen MO) a další správní orgány, které mají dané konkrétní oblasti, v nichž se zapojují v zajištění dostatečných prostředků a pracovní kapacity ke zdárnému čelení proti působení jednotlivých aktivit a zdokonalují se v čelení těmto aktivitám.

> *„Zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.“* [24, čl.1]

3.5.2 **Zpravodajské služby**

Základním posláním zpravodajských služeb je neustálý sběr informací a jejich vyhodnocování. Cílem tohoto sběru dat je získání uceleného a co nejpodrobnějšího přehledu o bezpečnostní situaci, jehož pomocí jsme schopni odhalit ohrožení zájmů

a bezpečnosti státu a jeho obyvatelstva. V případě identifikace zvýšených aktivit hrozeb narušujících bezpečnost státu a jeho obyvatelstvo, může nechat vláda posílit kapacity těchto služeb k zvýšení intenzity zpravodajské činnosti. V zpravodajských službách probíhá v rámci činnosti cyklický informační proces: zadání, sběr informací, zpracování a výsledek. Zákonná úprava v současné době neumožňuje zpravodajským službám aktivní zapojení do preventivních a reaktivních opatření k zajištění bezpečnosti státu. Vymezením činnosti zpravodajských služeb se v současné době zabývají tři hlavní zákony. Jedná se o zákon č. 153/1994 Sb., o zpravodajských službách ČR, dále o zákon č. 154/1994 Sb., o bezpečnostní informační službě a zákon č. 289/2005 Sb., o Vojenském zpravodajství. [25]

Bezpečnostní a informační služba

Jedná se o zpravodajskou instituci, která je řízena a kontrolována vládou ČR a působí na území ČR. Bezpečnostní a informační služba (dále jen BIS) je striktně apolitická, sloužící demokratickému státu a jeho občanům, kteří službu platí ze svých daní. Příslušníci BIS jsou vzhledem k faktu, že BIS je bezpečnostním sborem, ve služebním poměru. Z tohoto statutu mají oprávnění držet a nosit služební zbraň, kterou však mohou použít pouze k odvrácení hrozícího nebo trvajícího ohrožení v případě nutné obrany a krajní nouze, tak jak je umožněno každému občanovi ČR. Příslušníci mají služební hodnosti a k nim souhlasící služební označení, jelikož se jedná o represivní složku, tak nemohou nikoho zadržovat, vyslýchat či zatýkat. Veškeré informace, které BIS získá a ověří, předává prezidentu republiky, vládě (předsedovi vlády a jednotlivým ministrům), státním a policejním orgánům. Při své činnosti neustále dodržuje a důsledně dbá na lidská práva a svobody. [26]

Vojenské zpravodajství

Současné Vojenské zpravodajství (dále jen VZ) vzniklo v roce 2015 sloučením dvou služeb (rozvědné Vojenské zpravodajské služby a kontrarozvědného Vojenského obranného zpravodajství) a je součástí MO. Jeho vznik a působnost, však sahá již do doby první světové války, kde se prezentovala jako československé VZ. VZ je jednotnou ozbrojenou zpravodajskou službou, která jako jediná spojuje rozvědnou a kontrarozvědnou činnost. Jejím hlavním úkolem je vyhodnocování

získaných a shromážděných dat podstatných pro obranu ČR. VZ monitoruje chování zahraničních zpravodajských služeb zabývajících se obrannou oblastí a soustřeďuje se na aktivity a záměry s potenciálem ohrozit obranu a utajované skutečnosti ČR. Dále se podílí na zajištění kybernetické obrany ČR, k čemuž využívá Národní centrum kybernetických operací, které má za úkol v případě útoku v kyberprostoru zabezpečit ochranu nezbytné infrastruktury a civilního obyvatelstva. [27]

Úřad pro zahraniční styky a informace

Prvořadým cílem Úřadu pro zahraniční styky a informace (dále jen ÚZSI) je zajištění, získání včasných, kvalitních a objektivních informací pro orgány státní správy ČR a pro ústavní činitele, které jsou důležité pro ochranu a bezpečnost zahraničně politických a ekonomických zájmů ČR. ÚZSI je zpravodajskou službou snažící se získat informace zahraničního původu, které mohou být zachyceny a obdrženy i na území ČR. Jejím smyslem je chránit ČR proti hrozbám mezinárodního ražení. ÚZSI není součástí Ministerstvem vnitra, přestože spadá pod jeho rozpočet. Vnitřní organizace je upravována statutem, který schvaluje vláda. Zaměstnanci ÚZSI se řídí platnými právními a vnitřními předpisy, mezinárodními smlouvami, kterými je ČR vázáná a dalšími řídícími akty a usneseními, které upravují činnost úřadu. V neposlední řadě dodržují zaměstnanci také etický kodex. [28]

3.5.3 Orgány kybernetické bezpečnosti

Jak již bylo zmíněno, tak kybernetický prostor skýtá celou paletu pro nově vznikající hrozby, které ze zjevných důvodů nelze pomíjet. Pokud bychom tyto hrozby nereflektovali a kontinuálně se jim neučili čelit, měli by svým působením nežádoucí až katastrofické následky odrážející se v celé strategické infrastruktuře, která je v dnešní moderní době vysoce digitalizovaná, a tudíž vystavena možnému útoku více než tomu bylo dříve. Velmi obecně si zde představíme dva hlavní úřady zabývající se kybernetickou bezpečností a jejich podřízené a spolupracující instituce.

Národní bezpečnostní úřad

Národní bezpečnostní úřad (dále jen NBÚ) patří mezi ústřední úřady a zároveň i mezi úřady správní. Toto postavení NBÚ vyplývá z toho, že je orgánem

výkonné moci a ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti, a to již od svého počátku. Z tohoto postavení vyplývají dané pravomoci, kterými NBÚ disponuje, a kterých uplatňuje. Hlavním úkolem NBÚ je vydávání osvědčení (prověrek) nebo dokladů prokazujících bezpečnostní způsobilost osob, které dokládají, že u jejich držitelů nebylo zjištěno žádných skutečností, které by bránili přístupu a nakládání s utajovanými informacemi nebo vykonávání citlivých činností. Tímto prověřováním osob zajišťuje NBÚ bezpečné nakládání s utajovanými informacemi, a tím přispívá k ochraně důležitých informací pro obranné, vojenské, bezpečnostní, ekonomické a mezinárodně politické záměry a cíle ČR, a tím i k ochraně zdraví, života a majetku občanů. [29]

Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) vznikl 1. srpna roku 2017 a jedná se o ústřední správní orgán pro kybernetickou bezpečnost, která zajišťuje ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Mezi problematiku, kterou se NÚKIB dále zabývá je odpovědnost za problematiku veřejně regulované služby v rámci družicového systému Galileo. [30]

Výkonnou sekcí pod NÚKIB je Národní centrum kybernetické bezpečnosti, mezi jehož úkoly patří zejména prevence před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, informačním systémům základní služby, proti významným informačním systémům a vybraným informačním systémům veřejné správy. Dále spolupracuje s národními i mezinárodními organizacemi, s jejíž pomocí zabezpečuje kybernetický prostor vůči možným hrozbám. Mezi jejich aktivity patří i výzkum a vývoj, osvěta a vzdělávání v oblasti kybernetické bezpečnosti. Také zajišťují činnost Vládního CERT (Computer Emergency Response Team), který spolupracuje s národním CSIRT.cz (Computer Security Incident Response Team). Jedná se o týmy, které mají za úkol starat se o ochranu kritické informační infrastruktury a významných informačních systémů. Týmy musí být schopné účinně čelit bezpečnostním výzvám a efektivně reagovat na nastalé či předpokládané incidenty. Během řešení incidentů koordinují potřebné činnosti

a účelně vyvíjí činnost k předcházení těchto incidentů. V neposlední řadě mají tyto týmy i podstatnou úlohu ve vzdělávání širší veřejnosti v oblasti bezpečnosti na internetu. [31]

3.5.4 Centrum proti terorismu a hybridním hrozbám

Centrum proti terorismu a hybridním hrozbám (dále jen CTHH) vzniklo 1. ledna 2017 z rozhodnutí ministra vnitra na základě Auditu národní bezpečnosti 2016. Nutnost vytvoření centra tohoto typu, vyplývalo již ze schválené Bezpečnostní strategie 2015. Jedná se o analytické a komunikační pracoviště s minimálním počtem pracovníků. Hlavním úkolem CTHH je monitorování širokého spektra hrozeb a potencionálních incidentů napříč všemi možnými hrozbami. Mezi tyto hrozby řadíme například terorismus, extrémismus, narušování veřejného pořádku a páchání různých trestných činů nebo útoky na měkké cíle či monitoring dezinformačních kampaní se vztahem k vnitřní bezpečnosti státu. Na základě všech získaných informací CTHH vyhodnocuje detekované problémy a dává návrhy na legislativní řešení. Tato řešení CTHH se v nutném případě i zrealizují. Stejně jako jiné instituce se i CTHH zapojuje do osvěty a vzdělávání širší veřejnosti, k prohloubení informační bezpečnosti. [32]

3.5.5 Armáda ČR

V neposlední řadě nesmíme zapomenout ani na Armádu ČR (dále jen AČR), která má své pevné místo v zajišťování celkové bezpečnosti ČR. AČR spadá pod resort MO a hlavním velitelem ozbrojených sil je Prezident republiky. Základním stavebním kamenem AČR jsou její příslušníci. V řadách AČR je dle posledních dostupných informací 26 928 vojáků z povolání (dále jen VZP) a 3 615 příslušníků Aktivních záloh. Celkem má resort MO 35 127 zaměstnanců (do tohoto počtu spadají vojáci v činné službě a vojáci Aktivních záloh, státní a občanští zaměstnanci). Ideálním a cíleným stavem je, aby VZP byli správně a řádně motivováni, připravováni, vycvičeni a materiálně vybaveni k plnění úkolů při výkonu služby. AČR je nedílnou součástí nutnou k udržení suverenity státu a ochraně a obraně státních zájmů. V době nouzového stavu nebo stavu válečného se vytváří zvláštní struktury,

ve kterých je AČR hlavním výkonným prvkem a slouží k zajištění přímého řízení obrany. [17, 33]

Velitelství kybernetických sil a informačních operací

Velitelství kybernetických sil a informačních operací (dále jen VeKySIO) vzniklo 1. července 2019 se sídlem v Brně. VeKySIO spadá do taktické úrovně AČR spolu se Vzdušnými a Pozemními silami, a také Velitelstvím teritoria. VeKySIO může působit, jak nezávisle, tak společně nebo v součinnosti s ostatními druhy sil a VZ. Dále se podílí na civilně vojenské spolupráce tzv. CIMIC (Civil-Military-Interaction). Své operace řídí jak ve prospěch AČR, tak i k podpoře spojeneckých operací, pomocí monitorování a strategického plánování. Spolupracuje s ostatními prvky kybernetické bezpečnosti a obrany ČR. Vede rozmanité spektrum operací v kybernetickém prostoru včetně informačních a psychologických operací. Velitel VeKySIO poskytuje podporu nejvyššímu velení armády v oblasti strategické komunikace. [34]

> *„Úkolem kybernetických sil a informačních operací jako integrální součásti AČR je podpořit multidoménový přístup k vedení společných operací a přímo se do tohoto společného úsilí zapojit, kdy nejširší spektrum zainteresovaných subjektů jednoznačně chápe a podporuje význam kybernetického prostoru (jakožto nové operační domény) a vedení souvisejících informačních operací k prosazování zájmů České republiky v oblasti obrany.“* [35]

3.6 DIMEFIL

DIMEFIL (Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal) je zkratka pro sedm dimenzí vlivu, ve kterých je možné vést hybridní kampaň. Hybridní vedení konfliktů není nic nového. Nový je však rozsah a způsob, jakým se použité nástroje kombinují, aby bylo dosaženo strategického cíle. Původcem kampaně mohou být státní i nestátní aktéři, kteří se tímto působením mohou dostat do konfliktu s mezinárodním právem. Těchto sedm dimenzí vlivu lze libovolně kombinovat, dle povahy zájmů původců.

3.6.1 **D – Diplomacie/Politika**

V této dimenzi vlivu jde o různá oficiální prohlášení čelních představitelů působících ve veřejných funkcích státu. Ministři či diplomati a ostatní čelní představitelé dávají najevo svůj vlastní názor k určitým skutečnostem a událostem a počítá s tím, že příjemci této zprávy, kterými jsou zejména zahraniční subjekty a mocnosti budou na tuto informaci reagovat konkrétními a očekávanými kroky. Oficiálně je možné vystupovat proti nezákonným jevům v jiných zemích, kdy je širší veřejnosti nastíněno a ukázáno na nebezpečnost a neschopnost tamějších vlád účinně a včasně reagovat na projevy těchto jevů. Tímto poukázáním se dosáhne podpoření radikálních sil v zemi, kde se tyto jevy vyskytují nebo podpoření jiné země, která hodlá do dění zasáhnout.

3.6.2 **I – Informace**

Zde se setkáváme se silou vlivu, který přináší sdělovací prostředky a sociální sítě. V dimenzi informační moci se využívá sociálních sítí a masmédií k manipulaci a šíření dezinformací nebo k propagandě zájmových subjektů a jejich aktivit. Cílem těchto dezinformací a propagandy je snaha přesvědčit obyvatelstvo o určité skutečnosti, která má aktérům pomoci v budoucím bytí a jednání. Pokud se povede, aby byla veřejnost o skutečnosti přesvědčena (ovládáme veřejné mínění), lze poté využít jejího chování k ovlivnění plánovaných zámyslů, kterými mohou být například volby. Moc nad sdělovacími prostředky a moc získání prostoru v masmédiích nejsou to samé. Pokud ovládáme masmédia, můžeme lépe a efektivněji ovlivňovat prostor v těchto médiích. Pokud dostaneme dostatečný prostor ve sdělovacích prostředcích, který umíme i dostatečně využít, může stačit pouze správně použít kombinaci lží a pravd v oponentních názorech, abychom dosáhli žádaného výsledku. Lživé informace se šíří mnohonásobně rychleji než ty pravdivé, proto je velmi obtížné pokoušet se je vyvracet a vysvětlovat pravý význam informací, se kterými se manipulovalo. V prostředí sociálních sítí to platí dvojnásob, protože spojuje spoustu skupin smýšlejících na základě těchto zmanipulovaných informací. Díky utvrzování se ve vlastním názoru pomocí internetových diskuzí s podobně smýšlejícími jedinci v komunitách sociálních sítí následně extrémně ztěžuje oponentům vysvětlit či vyvrátit tuto informaci a uvést ji na pravou míru, a tím si zpět přiklonit veřejnost na základě jejího mínění. Důsledkem

takového využití masmédií a sociálních sítí může být i to, že se zde vůbec neodráží objektivní realita, ale je těmito médii a sítěmi přímo vytvořena.

Jedním z informačních nástrojů je Overtonovo okno (pojem vznikl podle autora této myšlenky – Joseph P. Overton).

„Overtonovo okno je způsob společensko-mediální manipulace, na konci, kterého je ve společnosti prosazeno to, co dříve nebylo myslitelné. Podle Overtona existuje pro každý společenský problém tzv. okno možností. V rámci něj lze o něm diskutovat tak dlouho až je společnosti nemyslitelné téma akceptováno, případně i legislativně ukotveno.“ [36]

Je třeba zdůraznit, že se nejedná o žádné klasické vymývání mozku, kdy se vtlouká konkrétní informace do zblbnutých, dokud není většinou přijata. Je zde zaměřeno spíše na určité cílové skupiny, které jsou k tomuto aplikování informací nakloněny. Overtonova okna jsou mnohem propracovanější, časově náročnější, ale mnohem, mnohem účinnější. S dostatkem času a nadvládou nad masmédii se dá prosadit skoro úplně cokoliv, ne-li všechno, co si lze představit. [36]

Overtonova okna mají šest fází:

- První fáze – nepřijatelné, ale mluvme o tom.
- Druhá fáze – desakralizace.
- Třetí fáze – nahrazení původního výrazu eufemismem a vytvoření podpěrného precedentu.
- Čtvrtá fáze – z možného do racionálního.
- Pátá fáze – popularizace.
- Šestá fáze – z kategorie populární do aktuální sféry politiky.

3.6.3 **M – Ozbrojené síly**

Do této dimenze patří obzvláště účast ozbrojených sil v aktivních operacích, ale i účast na národních a mezinárodních vojenských cvičeních, pořádání vojenských přehlídek, otevřené výhružky útokem (demonstrace moci v podobě nejrůznějších prohlášení o vstupu do jiné země) či účast v mírových misích apod.

Dále sem patří partyzánské operace vedené v utajení a dotované teroristické útoky, které jsou vedené anonymně nebo je z nich nařknuta jiná strana konfliktu, na kterou je pro útočící stranu výhodné daný agresivní čin svést. Mohou zde být zastoupeny i schválené legitimní vojenské operace, které jsou namířené třeba i proti těmto partyzánským a teroristickým aktivitám, přičemž v pozadí může být jedna a tatáž osoba či subjekt.

V rámci AČR působí pod kybernetickými silami jednotka 103. centra CIMIC/PSYOPS (Civil-Military-Interaction/Psychological Operations), která má za úkol reagovat na hrozby v kyberprostoru a prostředí informačních technologií. Cílem jednotky a armády je společný komplexní boj, který spočívá v činnosti všech druhů sil ve stejném čase ve všech operačních dimenzích. [37]

3.6.4 **E – Ekonomika**

V této dimenzi vlivu se využívá určitých forem nátlaku ekonomické povahy. Může docházet k uvalení embarga a cel na strategické suroviny nebo jinak významné komodity, důležité pro zájmovou stranu konfliktu. K docílení omezení množství těchto surovin a komodit, může být použito pod nejrůznějšími záminkami, které sníží nebo zpozdí dodávky, třeba i za cenu dočasného zhoršení situace na vlastním území či ve své vlastní zemi. Snížená produkce pro dané suroviny se dá vyvolat destabilizací klíčových odvětví (výrobní a zpracovatelské procesy podniků apod.), nebo znemožnění transportu z důvodu zamezení používání dopravních tras (třeba vyvoláním konfliktu na území států a subjektů, které jsou využívány k přesunu těchto surovin a komodit).

3.6.5 **F – Finančnictví**

Dimenze vlivu s instrumenty finančního trhu představuje silný nástroj (peníze, kapitál, zboží), který se dá využít hlavně k ovlivnění měnové politiky a bankovního sektoru. Zejména pak destabilizace měny a ovlivňování klíčových finančních institucí vedou k velmi negativním dopadům na státní zřízení nebo organizační subjekt. Avšak z důvodu současného silného propojení světových institucí, vyžaduje toto ovlivňování značně zvýšenou aktivitu při vynaložení potřebného úsilí a zajištění velkého množství zdrojů, aby bylo požadovaného úkonu docíleno. Menší úsilí a více pravděpodobná úspěšnost s narušením finančního trhu

se dá očekávat u otevřené ekonomiky menších subjektů a států, nebo u uzavřených ekonomik, u které se dá i lépe odhadnout a určit dopad a vliv použitých nástrojů.

3.6.6 **I – Zpravodajství**

V dimenzi zabývající se zpravodajstvím je zcela zjevné již z názvu, že zásadním zdrojem potřebným pro rozhodování při činění dalších kroků jsou informace získané prostřednictvím aktivit zpravodajských služeb. Těmito aktivitami se rozumí, že zpravodajské služby provádí různé analytické a operativní činnosti. Zejména špionáží nebo i kompromitací či vydíráním apod. Špionáž může vzejít vlastní infiltrací nebo získáním spolupracujících osob, které se podílejí na protistátní činnosti.

3.6.7 **L-Veřejný pořádek a právní stát**

Tato dimenze vlivu je útočníky využívána k rozvracení státního uspořádání a pořádku za pomoci využití nástrojů sloužících k podvratné činnosti. Tato činnost subverze spočívá zejména v ovlivňování skupin, které jsou nábožensky, sociálně nebo etnicky rozděleny ve společnosti a kastovány danými společenskými liniemi. Mezi těmito skupinami se lépe podněcují nepokoje, kdy probíhá podpora demonstrací, občanských konfliktů a různých stávek. Záměrně se vyvolávají drobnější potyčky, ozbrojené střety a rozdmýchávají se válečné konflikty. V daných lokalitách se zvyšuje kriminalita dodáváním zbraní a prodejem drog, což ještě více prohlubuje destabilizaci a demoralizaci v dané oblasti a vede až k tomu, že země může upadnout v chaos. Takto ovlivnitelné skupiny se tedy zejména nacházejí v zemích, které jsou velmi nábožensky založeny nebo mají nízkou životní úroveň, popřípadě jde o kombinaci těchto dvou skutečností. Dále se v této dimenzi vlivu využívá různých kriminálních a teroristických metod, jako jsou vydírání, zastrašování nebo únosy. Ohroženou skupinou, která lze lehce zmanipulovat je obzvláště nepracující mladá generace Středního východu a Afriky, ta je často i méně gramotná, a proto lehčeji ovladatelná.

Ozbrojené síly RF na území UA

Aktuálním příkladem hybridní hrozby kombinující více vlivů je tzv. „speciální vojenská operace“ ozbrojených sil RF na území UA. Prezident Putin tuto operaci odůvodňuje tím, že vojáci ruské armády bojují za životy a mír obyvatel v oblasti

Donbasu a za denacifikaci a demilitarizaci UA. Tím popírá, že jde o cílený útok na suverénní stát. Prezident Putin z pozice moci svého mandátu řídí kroky „speciální vojenské operace“ skrz sféru vlivu politiky, jakožto hlava státu a vrchní velitel. Pomocí řízení místních médií a sociálních sítí ovládá sféru vlivu informací a záměrně dezinformuje obyvatele vlastní země o dění a stavu na území UA. Výhružkami a demonstrací síly, která vyústila, až k aktivní vojenské operaci na území suverénního státu využívá sféru vlivu ozbrojených sil. Díky dodávkám ropy a zemního plynu, které se jsou distribuovány z RF, je využita sféra vlivu ekonomiky, kdy RF hrozí uzavřením dodávek těchto zdrojů a zároveň se dotýká i sféry finančnictví, jelikož si může v určité míře dirigovat ceny za tyto nerostné suroviny. Ekonomika a finančnictví jsou ovlivněny i sankcemi uvalenými na RF z důvodu tohoto nepřijatelného působení na území jiného státu. Sankce jsou znatelné zejména zmrazením finančních prostředků ruských institucí a oligarchů a odchodem zahraničních firem z ruského území a trhu. Dále se byli uvaleny sankce na sportovní činnosti (různá mistrovství světa), kdy jsou ruští sportovci a jejich týmy vyřazeni ze sportovních klání a nesmějí pořádat mezinárodní sportovní události.

RF se již dříve rozhodla chránit své obyvatele proti UA. Po ukrajinské revoluci v březnu 2014, vypukly ve značné části Donbasu nepokoje, které vyústily až do válečného konfliktu. V tomtéž roce obsadili proruští separatisté vládní budovy a prohlásili vytvoření dvou samozvaných nezávislých republiky. Těmi jsou Doněcká a Luhanská lidová republika. Tyto dvě oblasti byli 21. února 2022 uznané RF za legitimní. Od roku 2014 si boje mezi ukrajinskými silami a proruskými separatisti vyžádali více než čtrnáct tisíc lidských životů. [38]

4 METODIKA

V následujících kapitole provedu analýzu vybraných opatření působících v konkrétních doménách DIMEFIL. Bude vytvořena Tabulka 1, kde budou v horním řádku vypsaná konkrétní opatření a v levém sloupci jednotlivé sféry vlivu (DIMEFIL). Opatřením budou v tabulce označena písmeny A až E, dle pořadí, ve kterém budou v textu zmíněna. U každého popisu opatření bude písmeno k němu náležící zmíněno. Střed tabulky poté vyplní vyjádření „Ano“ a „Ne“, která řadí nebo neřadí dané opatření do dané sféry. Odpověď „ANO“ bude podbarvena zelenou barvu a odpověď „Ne“ červenu barvou. Po vyplnění tabulky, požadovanými údaji se ke každé situaci vyjádřím. Proč jsem tu a onu možnost zvolil nebo nezvolil do působení v dané doméně. Po zhodnocení všech možností, se opět vyjádřím ke konkrétním opatřením, na základě Tabulka 1 a navrhnu určité činnosti, které by měli lépe eliminovat možné hrozby.

4.1 Zvolená opatření

Pro analýzu je vybráno pět opatření, která cílí proti hybridnímu působení. Níže jsou tato opatření obecně popsána. Jedná se o činnost zpravodajských služeb, informovanost obyvatelstva, zabezpečení kyberprostoru, mezinárodní smlouvy a dohody a akceschopnost ozbrojených sil. Vybraná opatření jsou označena v Tabulka 1, dle pořadí od A do E.

4.1.1 Činnost zpravodajských služeb

Pod tímto opatřením rozumíme základní funkci zpravodajských služeb. Tou je schopnost odhalování hrozeb, které ohrožují zájmy státu. Detekce těchto hrozeb je možná díky neustálému sběru dat a informací (tzv. Situation and warning), které jsou následně vyhodnocovány. Cílem takto zpracovaných a vyhodnocených informací je získání co nejkomplexnějšího a nejpodrobnějšího přehledu o bezpečnostní situaci, díky němuž jsme následně schopni odhalit ohrožení zájmů a bezpečnosti státu a jeho obyvatelstva. Včasným odhalením ohrožení cílových zájmů se zajišťuje vyšší míra bezpečnosti státu. Toto opatření je v Tabulka 1 zastoupeno písmenem A.

4.1.2 Informovanost obyvatelstva

Společnost (obyvatelstvo) jakožto živý organismus má velmi silný a zásadní vliv na veřejné dění a tím i na bezpečnostní situaci. Šíření informací mezi lidmi probíhá nepřetržitě ve všech možných formách. Díky moderním informačním technologiím se navíc tento přenos informací rapidně urychlil. Předáváním informací ve velmi krátkém čase se zvětšil i rozsah pokrytí těmito informacemi. Z toho důvodu je velmi snadné se k informacím, ať již jsou pravdivé, pozměněné či zcela lživé, dostat a dále s nimi dle libosti nakládat. Proto je více než dost důležité, aby obyvatelstvo umělo tyto informace řádně zpracovat. Tímto zpracováním se zejména rozumí schopnost rozeznat původ a základ informací a schopnost je správně a efektivně použít. Opatřením informovanost obyvatelstva tedy myslím, jeho znalost a umění, jak s informacemi zacházet a nenechat se pouze ovlivňovat. Toto opatření je v Tabulka 1 zastoupeno písmenem B.

4.1.3 Kybernetická bezpečnost

V kyberprostoru se vytvářejí specifické a nové hrozby, které se prolínají napříč všemi dimenzemi moci. Denním používáním moderních technologií a pohybem v tomto prostředí jsme neustále vystaveni možnému působení těchto hrozeb. Informace a údaje se zde šíří abnormálně rychle v reálném čase. Tím pádem jsou okamžitě k dispozice, kdekoliv a pro kohokoliv, kdo má přístup k informačním technologiím a sociálním sítím, což je dnes díky rozmachu a dostupnosti, těchto prostředků valná část obyvatelstva. Díky provázanosti a komplexnosti kybernetického prostředí představuje jeho narušení velmi závažnou bezpečnostní hrozbu. Nejčastějšími hrozbami v kyberprostoru je pokus o exfiltraci dat nebo pokusy o narušení bezpečnostních a informačních systémů jak vládních, tak i nevládních organizací. Exfiltrací se pokouší útočník získat citlivá data a informace, kterými je následně schopen zdiskreditovat cíl svého útoku. Aktivitami snažícími se narušit bezpečnostní a informační systémy organizací, ale i jednotlivců mohou být různé pokusy o vyřazení těchto systémů. Cílem a důsledkem je pro útočníka stav, kdy bude subjekt zájmu neschopen používat nebo ovládat potřebné prostředky k plynulému chodu své činnosti a bude odříznut i od prostředků, kterými by mohl hrozbám zamezit. Toto opatření je v Tabulka 1 zastoupeno písmenem C.

K zabezpečení bezpečnosti v kyberprostoru využíváme tří pilířů „CIA“ (Confidentiality Integrity, Access). Prvním je důvěrnost, pomocí které se snažíme udržet potřebná tajemství a zajistit, že ke složkám a účtům mají přístup pouze osoby, které jsou k tomu autorizované. Druhým je integrita, jejíž cílem je ochránit data a obsah v takovém stavu, v kterém jsme je zanechali a ve stavu v jakém ho vyžadujeme mít. Jde o to, aby nikdo nemanipuloval s naším obsahem, vkládáním, odstraňováním nebo pozměňováním dat a informací. Třetím pilířem je přístup. Je potřeba zajistit, abychom měli ke svým systémům a datům kdykoliv přístup. Snažíme se předcházet případům, kdy nám je z různých důvodů zamezeno se ke svým údajům dostat a používat je. K zamezení přístupu může například dojít pomocí ransomware, kdy jsou naše systémy napadeny a následně zašifrovány, důsledkem čehož je nejsme schopni používat. [39]

4.1.4 **Mezinárodní smlouvy a dohody**

Toto opatření spočívá v zabezpečení a zajištění spolupráce na základě smluv a dohod mezi ČR a jinými státy nebo mezinárodními organizacemi. Tato spolupráce může být v rámci těchto uzavřených smluv a dohod použita na jakýkoliv zájem a k dosažení nejrůznějších prostředků a surovin, které se ke konkrétnímu zájmu vztahují. V těchto dokumentech se dva či více mezinárodně právních subjektů dobrovolně a záměrně dohodnou na určité pomoci či spolupráci v oblastech a případech, které jsou předmětem těchto dohod. Stěžejními jsou oblasti hospodářské, ekonomické, finanční, politické, ale i spolupráce na úrovni ozbrojených složek a sil a spolupráce Integrovaného záchranného systému při likvidačních a záchranných pracích větších rozsahů vyžadujících mezinárodní pomoc nebo probíhajících v přesahu území ČR. Toto opatření je v Tabulka 1 zastoupeno písmenem D.

4.1.5 **Akceschopnost ozbrojených sil**

K zabezpečení obrany území státu a jeho svrchovanosti je zapotřebí mít plně funkční a plně připravené ozbrojené síly a prostředky, pomocí kterých jsme schopni se bránit, čelit a zamezit možným ohrožením důležitých a klíčových zájmů ČR. Základním stavebním prvkem každé takto organizované struktury jsou její jedinci, tvořící její personál. V tomto případě tedy VZP, kteří přestavují páteř ozbrojených sil. Akceschopnost těchto sil závisí na znalostech, přípravě, materiální a technické

vybavenosti (také na počtu personálu, výstroje a výzbroje, techniky a ostatních potřebných prostředků), kterými disponuje a je schopná je adekvátně a efektivně využívat a používat k docílení požadovaného cíle vedeného k ochraně hájených zájmů důležitých pro integritu a uspořádání ČR a jejich spojenců. Toto opatření je v Tabulka 1 zastoupeno písmenem E.

5 VÝSLEDKY

V této kapitole je vypracována Tabulka 1 - Zařazení vybraných opatření do sfér DIMEFIL (dále jen „Tabulka 1), která uvádí, do kterých sfér moci jsou zařazena vybraná opatření proti hybridním hrozbám. Na základě toho se tedy jednotlivé zařazení do domén změní a vysvětlí, proč bylo takto učiněno. Následně jsou navržena opatření, která mohou dále eliminovat činnost hybridních hrozeb ve vybraných příkladech, a zefektivnit způsob čelení těmto hrozbám.

Tabulka 1 - Zařazení vybraných opatření do sfér DIMEFIL

Zařazení vybraných opatření do sfér DIMEFIL	A	B	C	D	E
Diplomacie	Ano	Ano	Ano	Ano	Ano
Informace	Ano	Ano	Ano	Ne	Ne
Ozbrojené síly	Ne	Ne	Ano	Ano	Ano
Ekonomika	Ne	Ne	Ano	Ano	Ne
Finančnictví	Ne	Ne	Ano	Ano	Ne
Zpravodajství	Ano	Ne	Ano	Ano	Ano
Veřejný pořádek a právní stát	Ano	Ano	Ano	Ne	Ne

5.1 Vliv opatření

Na základě údajů z Tabulka 1, rozeberu a popíšu, proč dané opatření působí na konkrétní sféry vlivu.

5.1.1 Diplomacie

Činnost zpravodajských služeb

V doméně vlivu diplomacie, mají aktivity zpravodajských služeb, dle Tabulka 1 své určité uplatnění. Díky činnosti související se sběrem a vyhodnocováním dat a informací, mají významný vliv pro řízení a strategie vedené státem. Na základě shromážděných dat a informací vytvářejí ucelený a komplexní přehled bezpečnosti státu a díky tomu jsou schopné odhalit ohrožení zájmu a bezpečnosti státu a obyvatelstva ČR. Do této sféry vlivu jsou zpravodajské služby zařazeny i proto, že zprávy a hlášení týkající se bezpečnostní situace jsou předávány v rámci obeznámení se situací ke konkrétním ministerstvům, ministrům, vládě, premiérovi a prezidentu ČR. Tyto řídící orgány na základě těchto informací rozhodují a provádí potřebné kroky k posílení, zamezení a zabezpečení strategických a klíčových zájmů, které mohu být dle těchto informací ohrožené nebo minimálně předmětem nějakých zájmů ofenzivních stran, které mají snahu nám uškodit.

Informovanost obyvatelstva

Veřejně dostupné informace, mají významný vliv na rozhodování obyvatelstva. Tabulka 1 proto řadí informovanost obyvatelstva mezi opatření působící na tuto sféru. Veřejné mínění je důležitým aspektem pro rozhodovací proces v demokratickém státě. Občané si své vládní zástupce volí ve veřejných volbách, kde se rozhoduje právě na základě informací, které se k nim dostávají. Svoboda názoru a volby, při použití dezinformací a lživých zpráv, se může obrátit proti veřejným i státním činitelům či jejich organizacím. Pokud je útočník schopen šířit dezinformace a informace kompromitující subjekty zájmů, může ovlivnit například právě volby nebo hlasování týkající se podstatných činností a projektů. Pokud navíc útočník umí s informacemi opravdu dobře nakládat, nelze většinou určit zdroj těchto informací, totožnost útočníka nebo skupiny útočníků. Z výše zmíněného vyplývá, že je velmi důležité, aby se k občanům dostávaly

co nejrelevantnější informace od ověřených zdrojů, které by neměly být, tak snadno zmanipulovatelné.

Kybernetická bezpečnost

Provozováním velkého množství aktivit přes informační technologie se každý uživatel vystavuje možnému nebezpečí spojeného s hrozbou napadení v kybernetickém prostředí (hackerské útoky, ransomware apod.). Tabulka 1 řadí kyberprostorovou bezpečnost k opatřením působících v této doméně. Zejména kvůli faktu, že spousta vládních systémů a aplikací se nachází právě v tomto prostředí. A nejedná se pouze o komplexní systémy, cílem útoků se mohou stát profily vládních činitelů na sociálních sítích, jejich služební i civilní e-mailové schránky a jiné aplikace, pomocí nichž komunikují. Při neochraňování svých digitálních dat, může dojít nejen k jejich ztrátě smazáním či krádeží, ale i k nežádoucí manipulace, kdy jsou data a informace pozměněna, a tím mohou daný cíl útoku značně poškodit. Pomocí exfiltrovaných dat se dají zájmové subjekty přimět ke spolupráci, pod formou nátlaku (vydírání, výhružky), díky držení citlivých informací, které subjekt mohou kompromitovat. Toto nedobrovolné spojenectví může vést k podvratné činnosti proti státu. Dále mohou zcizená data obsahovat informace, které by se neměla dostat na veřejnost a mohou ohrozit bezpečnostní systém a situaci státu. Všechna citlivá a soukromá data se musí řádně zabezpečit proti zneužití a ztrátě.

Mezinárodní smlouvy a dohody

V rámci tohoto opatření se obecně jedná o smlouvy a dohody zajišťující diplomatické styky s aliančními spojenci a jinými spřátelenými státy. V Tabulka 1 je toto opatření zahrnuto, neboť existuje řada smluv mezi ČR a dalšími státními subjekty a mezinárodními organizacemi, které ustanovují diplomatické vztahy a vazby. V této dimenzi moci se může jednat například o Chartu OSN, kde je stanoveno vzájemné nevměšování do politických věcí členských států nebo Vídeňská úmluva o diplomatických stycích, která vymezuje pravomoci a činnost zástupců vysílajících stran na území států přijímacích. [40]

Akceschopné ozbrojené síly

Ozbrojené síly jsou dalším opatřením, které Tabulka 1 určuje do působení sféry vlivu diplomacie. Základním předpokladem k zabezpečení suverenity a územní celistvosti státního zřízení, je mít plně funkční ozbrojené síly, které jsou schopné efektivně a včasně reagovat na blížící se a potenciální hrozby. AČR vykonává činnost k obraně a ochraně státních zájmů a obyvatel ČR. Jak již bylo zmíněno, tak Vrchním velitelem ozbrojených sil je prezident republiky, což je přímá spojitost s politickým spektrem. Finance na AČR jdou ze státní pokladny, tudíž je placena z peněz daňových poplatníků, občanů ČR. K zajištění řádné funkce ozbrojených sil je zapotřebí mít dostatek personálu, prostředků a techniky, spolu s dostatečným finančním zajištěním nutným k modernizaci a opravám v rámci připravenosti AČR.

5.1.2 Informace

Činnost zpravodajských služeb

Tabulka 1 určuje, že zpravodajské služby působí v dimenzi moci informace. Tyto služby neustále sbírají a vyhodnocují data a informace. Proces tohoto získávání dat je: zadání, sběr dat, vyhodnocení a výsledek. Na základě takto shromážděných dat a informací vytvářejí podrobný a komplexní přehled o bezpečnostní situaci státu. Pomocí vytvořeného přehledu jsou schopné odhalit ohrožení zájmu a bezpečnosti státu a obyvatelstva ČR. Zpravodajské služby si dokážou získávat relevantní informace z důvěryhodných zdrojů. Jsou schopné si ověřit původ konkrétních informací a dat a umějí je správně vyložit a pochopit. Subjekty, které dále pracují s informacemi, jenž jim zpravodajské služby poskytují, v ně mají plnou důvěru.

Informovanost obyvatelstva

Informace dostupné z masmédií a sociálních sítí, mají významný vliv na rozhodování obyvatelstva. Informovanost obyvatelstva je na základě Tabulka 1 zařazena do působení dimenze moci informace. V dnešní době je snazší získat velké množství informací. Záměrem uživatele je umět si vyselektovat a poznat podstatné informace od těch méně důležitých, což dost uživatelů podceňuje a neumí s daty pracovat efektivně.

Kybernetická bezpečnost

Tabulka 1 řadí kyberprostorovou bezpečnost k opatřením působícím v doméně Informace. V dnešní době se většina informací šíří pomocí internetu, sociálních sítí a aplikací, kterými jsou vybaveny informační technologie. Díky přísunu obrovského množství informací v reálném čase, se k uživateli dostávají pravdivé, lživé i upravené informace najednou. Pro běžného uživatele může být náročné se orientovat a rozpoznat pravdivost informací, které se k němu dostaly. Z tohoto důvodu je potřeba zamezit přísunu dezinformací k uživateli. K eliminaci dezinformací a šířených lží může sloužit blokace nebo zamezení přístupu nežádoucích skupin do kybernetického prostředí. Například web Sputnik, distribuující informace, které jsou cíleně upravené, aby podporovaly ruskou propagandu. Nejedná se pouze o formu, kterou informují webové stránky a sociální sítě, ale i informace zaslané na soukromé či firemní e-mailové schránky, které se nás pokoušejí ovlivnit. Kromě nevyžádaných informací a dezinformací, jsou tyto e-mailové zprávy hrozbou z důvodu přenosu počítačových virů. Po otevření může dojít buď ke ztrátě informací, nebo k zamezení přístupu k našim informacím. Dále k nežádoucímu šíření soukromých a citlivých zpráv a údajů, které byli těmito počítačovými viry získány. Z těchto zmíněných důvodů je důležité dbát na řádné zabezpečení kyberprostoru.

Mezinárodní smlouvy a dohody

Mezinárodní smlouvy a dohody nepůsobí na základě Tabulka 1 jako opatření vhodné v dimenzi vlivu informace. Občané ČR nevyužívají mezinárodní smlouvy a dohody v takové míře, která by jim pomáhala v dalším rozhodování.

Akceschopné ozbrojené síly

Podle Tabulka 1 se opatření akceschopných ozbrojených sil přímo netýká dimenze moci informace. V případě možné hybridní hrozby ze sféry informace, není možné toto nebezpečí eliminovat pomocí síly za použití sil a prostředků AČR.

5.1.3 Ozbrojené síly

Činnost zpravodajských služeb

Na základě Tabulka 1 nepůsob zpravodajské služby ve sféře vlivu ozbrojené sly. VZ sice patř pod MO, ale nen součást ozbrojených sil. Zpravodajské služby zatm nemaj pravomoci, které by jim umožnily aktivn zapojen do prevence a reakce proti nepřátelskému jednán jimi vypozorovaného.

Informovanost obyvatelstva

Jak je v Tabulka 1 uvedeno, tak toto opatřen nepůsob v dimenzi moci ozbrojených sil. V případě nutnosti využit ozbrojených sil se veřejnost do jejich aktivit nezapojuje. Aktivity k ochraně a obraně bezpečnostních zájmů jsou řzeny profesionáln velen.

Kybernetická bezpečnost

Ozbrojené sly jako ostatn státn instituce použvaj moderních technologi připojených k internetové sti a dalš systémy vyskytujících se v kybernetickém prostřed Proto je v Tabulka 1 kyberprostorová bezpečnost jedn z opatřen působícího ve sféře vlivu ozbrojené sly. Intern informace šířené v rámci plněn úkolů AČR, Hradní stráže a Vojenské kanceláře prezidenta republiky, jsou většinou citlivé, důvěrné nebo tajné. Kvůli povaze těchto informac se mus velmi důsledně dbát na jejich ochranu a zabezpečen proti zneužit V posledních době je velmi aktivní hrozbou napadán služebních e-mailových schránek personálu MO a příslušníků ozbrojených sil. Pod velmi důkladným dohledem, mus být zabezpečen systému použvaných k obraně a ochraně státu. Například odpojen nebo zneužit systému protivzdušné obrany nepřátelskými aktéry, by znamenalo kritickou hrozbu pro bezpečnostní stav na bráněném územ

V rámci taktické úrovně spadajících pod AČR, vykonává svou úlohu VeKySIO. Toto velitelstv působ jak nezávisle, tak společně s Vojenským zpravodajstvím nebo spolupracuje s ostatními druhy sil. Dokáže vést široké spektrum operac v kybernetickém prostřed V kybernetickém prostřed působ nepřetržitě a zajišťuje podporu k ochraně před kybernetickými, informačními a hybridními

hrozbami, vedou operačn komunikaci, chrán své síly a prostředky a koordinuj informačn operace. Podstatným aspektem je poskytován klíčových informac operačnímu veliteli. [34]

Mezinárodní smlouvy a dohody

Opatřen v podobě mezinárodních smluv a dohod je na základě Tabulka 1 opatřením, které působ na dimenzi moci ozbrojených sil. Zabezpečen vojenské pomoci je zmíněno v rámci aliančních dokumentů a hraje důležitou roli k ochraně a obraně zájmů, jak ČR, tak i NATO a EU, se kterými zastáváme stejné hodnoty. Jako nejdůležitější a v současné době diskutovanou zmíním Washingtonskou smlouvu. Tu podepsalo v roce 1949 deset států. Jejím hlavním cílem bylo vytvořit spolupracující koalici, která by si navzájem pomohla v reakci na riziko, které představoval Sovětský svaz. Washingtonská smlouva je zakládajícím a hlavním dokumentem Severoatlantické aliance, a přistoupen k této smlouvě podepisuj všechny členské státy. ČR tedy podepsala toto přistoupen v roce 1999. Nejprobíranějším bodem je v současné době článek 5 – o kolektivní obraně. [41]

> *„Smluvní strany se dohodly, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem, a proto se dohodly, že dojde-li k takovémuto ozbrojenému útoku, každá z nich, uplatňujíc právo na individuální nebo kolektivní sebeobranu uznané článkem 51 Charty OSN, pomůže smluvní straně nebo stranám takto napadeným tím, že neprodleně podnikne sama a v součinnosti s ostatními stranami takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a zachovat bezpečnost severoatlantického prostoru. Každý takový útok a veškerá opatření učiněna v jeho důsledku budou neprodleně oznámena Radě bezpečnosti. Tato opatření budou ukončena, jakmile Rada bezpečnosti přijme opatření nutná pro obnovení a zachování mezinárodního míru a bezpečnosti.“* [41, čl. 5]

Akceschopné ozbrojené síly

Podle Tabulka 1 řadíme opatřen akceschopných ozbrojených sil do dimenze moci ozbrojené síly. Je zcela jasné, že sem náleží, protože toto opatřen je pevnou součást této domény. Do činnost ozbrojených sil v této doméně patř účast

na národních a mezinárodních vojenských cvičeních, pořádání různých vojenských přehlídek, účast v mírových misích, ale hlavně aktivní zapojení ve vojenských operacích. Dále se dá síla a moc demonstrovat v podobě nejrůznějších prohlášení a výhružek (například invazivním vstupu do jiné země). Jsou zde zastoupeny i legitimní vojenské činnosti namířené k potlačení teroristických či partyzánských aktivit, které ohrožují zájmy a bezpečnost státu a jeho obyvatelstva.

5.1.4 Ekonomika

Činnost zpravodajských služeb

Tabulka 1 udává, že zpravodajské služby nepůsobí ve sféře vlivu ekonomika. Činnosti a procesy sběru dat a informací nemají v rámci působení přes tuto doménu vliv na probíhající ekonomické aktivity.

Informovanost obyvatelstva

Ani informovanost obyvatelstva není na základě Tabulka 1 opatřením působícím v dimenzi moci ekonomika. Získané a zpracované informace slouží k tomu, abychom si udělali přehled o současném stavu dění, nemají vliv na naši ekonomickou situaci.

Kybernetická bezpečnost

Jako každý jiný subjekt se i státní podniky a soukromé firmy zabývající se výrobou, zpracováním nebo distribucí různých surovin a komodit, pohybují v rámci uzavírání obchodu v kybernetickém prostředí. Proto je kyberprostorová bezpečnost dle Tabulka 1 zařazena do domény ekonomika. Tyto subjekty mají vytvořené elektronické systémy pro různé evidence pohybu, nákupu, prodeje a jiných potřeb. Přes dispečery a jejich komunikační a informační sítě řídí dopravu těchto surovin a předávají si informace o poloze a stavu těchto transportů. Narušením chodu systémů řídících logistiku nebo výrobu produktů nepřátelskými aktivitami, může dojít k zdržení nebo pozastavení dodávek zájmových komodit, a tím narušit chod subjektů, které jsou na těchto komoditách závislé nebo je v menší či větší míře potřebují ke své činnosti. Opět je tedy nezbytné dbát na řádné a kvalitní zabezpečení svých dat a informací nacházejících se v kybernetickém prostředí.

Mezinárodní smlouvy a dohody

Podle Tabulka 1 jsou mezinárodní smlouvy a dohody opatřením, které působí na sféru moci ekonomika. ČR má po celém světě smluvní partnerské státy, které s ní spolupracují v rámci hospodářství, průmyslu, energetiky, různých druhů dopravy apod. Dokumenty řadícími se do těchto smluv jsou například: smlouvy o hospodářské a průmyslové spolupráci; smlouvy o hospodářské, průmyslové a technické kooperaci; dohody o mezinárodní silniční dopravě; dohody o letecké dopravě a jiné. Smlouvy a dohody jsou sepsané s konkrétními státy. [42]

Akceschopné ozbrojené síly

Tabulka 1 neřadí opatření akceschopných ozbrojených sil do sféry vlivu ekonomika. V případě mimořádné události antropogenního původu ve formě ekonomických hrozeb, nemají akceschopné ozbrojené síly prostředky k jejich zamezení a schopnost k ovládnutí situace.

5.1.5 Finančnictví

Činnost zpravodajských služeb

Tabulka 1 ukazuje, že zpravodajské služby nepůsobí v dimenzi moci finančnictví. Při možných hrozbách týkajících se měny a bankovních institucí nejsou aktivity těchto služeb související se sběrem a vyhodnocováním dat, podstatné pro jejich řešení.

Informovanost obyvatelstva

Stejně tak Tabulka 1 mluví o opatření informovanosti obyvatelstva, které v této doméně také nepůsobí. Získané a zpracované informace slouží k tomu, abychom si udělali přehled o současném stavu dění, nemají vliv na naši finanční situaci.

Kybernetická bezpečnost

Tabulka 1 dokládá působení kyberprostorové bezpečnosti v této dimenzi moci. Bankovní sektor je jedním ze subjektů kritické infrastruktury. Opatření zabezpečení kyberprostoru je proto nezbytné. Většina finančních transakcí probíhá v kybernetickém prostředí. Bankovní a finanční instituce spravují a používají

rozsáhlé spektrum elektronických systémů (elektronické bankovnictví, smart klíče aj.) V současné moderně se vyvíjející době, stále více lidí používá moderních technologií k zabezpečení a vyřízení svých finančních náležitostí. Cílem útoku, tak nemusí být organizace nebo státní subjekt, ale i konkrétní zařízení jedince (mobilní telefon, přenosný počítač, tablet apod.). Základem je tedy mít zabezpečené své zařízení, které ke zprostředkování využíváme a své uživatelské účty. Častým útokům a hrozbám čelí samotné instituce bankovních domů. Napadením jimi používaných systému může dojít k destabilizaci měny nebo finančním ztrátám velkého rozsahu, který by byl schopný ohrozit bezpečnostní situaci státu. Dalším finančním subjektem je burza, kde se neustále převádí obrovské množství finančních prostředků. Zajištění chráněného a bezpečného přístupu na burzu a následně i bezpečnostního prostředí, ve kterém se aktivita uskutečňuje je podstatné pro uhlídání svých investic. To samé platí u jakékoliv instituce zacházející s financemi v kyberprostoru. Mít bezpečný přístup ke svým účtům a finančním prostředkům je jednou z hlavních činností prováděných v rámci zajištění kybernetického prostředí.

Mezinárodní smlouvy a dohody

V doméně finančnictví je v Tabulka 1 zařazeno toto opatření mezinárodních smluv a dohod, jako působící. Tok finančních prostředků za hranice státu je zcela běžný a probíhá takřka neustále. Tyto finance proudí jako náklady na provoz, nákup, investice a apod. v rámci obchodu mezi firmami, institucemi nebo i jednotlivými subjekty a jejich zahraničními protějšky, ale i obráceně jako zisky z těchto aktivit. Jako příklad mezinárodních dohod můžeme zmínit dohody o podpoře a vzájemné ochraně investic, které jsou sepsané a uzavřené s jednotlivými státy. Tyto konkrétní smlouvy lze nalézt na stránkách Ministerstva financí ČR. [43]

Akceschopné ozbrojené síly

Tabulka 1 neřadí opatření akceschopných ozbrojených sil do dimenze moci finančnictví. V případech ohrožení investic nebo stability měny, je použití sil a prostředků ozbrojenými silami bezpředmětné a nevedlo by ke stabilizaci problému.

5.1.6 Zpravodajství

Činnost zpravodajských služeb

Jelikož zpravodajství je základním úkolem zpravodajských služeb, tak je jasné, že i na základě Tabulka 1 bude činnost zpravodajských služeb zařazena do působení v dané dimenzi moci. Jejich primárním úkolem je neustálý sběr informací a jejich vyhodnocování. Výstupní data a informace tohoto sběru mají vytvořit ucelený a co nejpodrobnější přehled o bezpečnostní situaci, díky kterému jsme schopni odhalit ohrožení zájmů a bezpečnosti státu a jeho obyvatelstva. Na základě detekce zvýšeného množství aktivit hrozeb, které jsou schopné narušit bezpečnost státu a jeho obyvatelstvo, má vláda kompetence, kterými může posílit kapacity zpravodajských služeb ke zvýšení intenzity zpravodajské činnosti. Zpravodajské služby se v současné době nemohou aktivně zapojit do reaktivních a preventivních opatření k zajištění bezpečnosti státu.

Informovanost obyvatelstva

Z údajů z Tabulka 1 vyplývá, že informovanost obyvatelstva nepůsobí v dimenzi moci zpravodajství. Veřejné mínění neovlivňuje činnost zpravodajské služby. Zpravodajské služby pracují s informacemi, které procházejí důkladnou analýzou. U těchto informací jsou schopné určit naléhavost/závažnost, která má být sdělením, a hlavně jejich původ. Díky cyklickému procesu se použijí pouze relativní informace.

Kybernetická bezpečnost

Dle Tabulka 1 je toto opatření, které působí v rámci dimenze zpravodajství. Stejně jako u ostatních zmíněných opatření, se i zde provádí velká část úkonů a aktivit v kybernetickém prostředí. Únik nebo odcizení dat ze zpravodajských aktivit by mohlo znamenat přímé ohrožení bezpečnosti státu. Velká část informací podléhá některému ze stupně utajení. Může se jednat o informace osob v utajení a jejich činnosti nebo budoucích strategických cílů a podobně. Tyto informace se předávají a organizují ve vysoce postavených strukturách ČR. Jako vždy je v takto významných institucích důležité nastavit dostatečné a kvalitní kybernetické zabezpečení.

Mezinárodní smlouvy a dohody

Dle Tabulka 1 má v této doméně vlivu opatření ve formě mezinárodních smluv a dohod význam. Konkrétně jde o výměnu utajovaných informací a jejich následnému užívání. Vzhledem k citlivosti údajů, které se v těchto informacích vyskytují, je bezprecedentní povinnost tyto údaje řádně zabezpečit a ochránit proti zneužití. Příprava návrhu a následné uzavírání těchto specifických smluv má na starosti jako ústřední správní úřad NBÚ. Konkrétně se jedná o mezinárodní smlouvy o výměně a vzájemné ochraně utajovaných informací, které jsou dohodnuté s jednotlivými státy, s nimiž spolupracujeme v rámci těchto výměn.

„Při stanovování priorit v této oblasti Úřad vychází z praktické potřeby výměny utajovaných informací s konkrétními státy a z potřeby zajistit těmto informacím odpovídající ochranu. Sjednávání smluv o ochraně utajovaných informací je zcela v souladu se zahraničně politickými zájmy ČR stejně jako se závazky, které pro Českou republiku vyplývají z členství v EU a NATO.“ [44]

Akceschopné ozbrojené síly

Vzhledem k existenci VZ je v Tabulka 1 toto opatření zařazeno do působení ve sféře vlivu zpravodajství. VZ je jednotná ozbrojená složka pod MO a spojuje rozvědnou a kontrarozvědnou činnost. Jako u ostatních zpravodajských služeb je jejím hlavním úkolem VZ získávání a shromažďování informací, které následně vyhodnocuje. Dále monitoruje chování zahraničních protějšků a vyhledává informace a aktivity, které mohou být použity se záměrem ohrozit utajované skutečnosti a obranu ČR.

5.1.7 Veřejný pořádek a právní stát

Činnost zpravodajských služeb

Zpravodajské služby jsou z větší části službou pro civilní sektor, a proto jsou podle Tabulka 1 opatřením, které má vliv na doménu veřejné pořádek a právní stát. Jimi shromážděná data získána sběrem informací, se po vyhodnocení mohou použít k zabezpečení veřejného pořádku. Sdělení, která nám mohou být poskytnuta, mohou následně přispět k ochraně právního státu a posilovat veřejný pořádek. Řádná činnost zpravodajských služeb má proto na tuto doménu silný vliv. V případě

nekontrolovatelného šíření dezinformací, by mohlo docházet k narušení pořádku v podobě nepokojů, demonstrací a fyzických potyček. Mít správná, pravdivá, podložená a dohledatelná data je žádoucím cílem zpravodajských služeb.

Informovanost obyvatelstva

Tabulka 1 řadí opatření informovanosti obyvatelstva do působení ve sféře vlivu veřejný pořádek a právní stát. Obyvatelstvo má spoustu možností, kde a jak získávat informace. Ne všechny tyto informace jsou, však pravdivé nebo založené na reáliích a může vzniknout šíření dezinformací. Předáváním nebo manipulováním informací a dat, dochází k jejich zkreslení nebo úplné změně neseného sdělení, čímž vzniká špatný úsudek na popisovanou událost či čin. Optimálně by občané měli pracovat s informacemi, které se dají ověřit a získat zdroj původu. Čím více podložených informací máme, tím by měli být důvěryhodnější.

Kybernetická bezpečnost

Opatření kyberprostorové bezpečnosti je na základě Tabulka 1 též součástí působící v této doméně. Jak již bylo několikrát zmíněno, obrovská část aktivit se uskutečňuje v a prostřednictvím kybernetického prostředí. Sociální a internetové sítě, softwarové aplikace, elektronické zabezpečovací systémy a mnoho dalších prostředků vyskytujících se v kybernetickém prostředí je vystaveno ohrožení formou hackerských útoků. Spousta institucí má své aktivity online. Do této skupiny patří třeba vzdělávací instituce všech úrovní, sociální a zdravotní zařízení, různé úřady, veřejná správa a další. Například nabouráním systému nějaké nemocnice může dojít ke komplikacím, které mohou vést i ke ztrátám na životech. Jsou nefunkční rezervační systémy, nejsou dostupné údaje o pacientech, nelze provádět komplikovanější operační zákroky vyžadující moderní technologie. Data a informace mohou být buď pouze nedostupná, nebo smazána či dokonce odcizena. Nebo cílí na vzdělávací instituce, které mohou vést nějaký výzkum. Ten buď chtějí útočníci zastavit, nebo zneužít. Útočníci mohou vyžadovat za navrácení kontroly nad systémy nebo navrácení odcizených dat různé požadavky. Většinou se jedná o peněžní prostředky, nebo mohou za navrácení dat vyžadovat úkony, které jsou v jejich zájmu a instituce je schopna tyto úkony zajistit. Vzhledem k těmto okolnostem je nezbytně nutné vynaložit dostatečné úsilí k zabezpečení a ochraně kybernetického prostředí,

ve kterém se instituce vyskytují, neboť vynaložené finanční prostředky na zabezpečení jsou mnohonásobně nižší než ty, které se vynaloží na odstranění a vyřešení škod.

Mezinárodní smlouvy a dohody

Tabulka 1 říká, že opatření mezinárodních smluv a dohod, není v působení na sféru moci veřejného pořádku a právního státu. Toto opatření se týká aktivit a spolupráce probíhající mezi ČR, státy, a státními organizacemi a jejich zahraničními protějšky.

Akceschopné ozbrojené síly

Podle Tabulka 1 ani toto opatření nepůsobí v dimenzi vlivu veřejný pořádek a právní stát. Ozbrojené síly jsou jako poslední možnost, která by byla použita k udržení veřejného pořádku, a to v případě vyhlášení nouzového nebo válečného stavu. Nebo při mimořádných událostech větších rozsahů, jakožto posílení složek integrovaného záchranného systémů. Za normálních okolností by se na dodržování pořádku podíleli ozbrojené sbory a likvidačním a záchranným pracím sbory záchranné.

Všechna vybraná opatření začleněná do tabulky byla analyzována v rámci domén spektra DIMEFIL. Následně byla odůvodněna. V rámci hybridního působení při konkrétní hrozbě, se však mohou konkrétní opatření týkat i dalších domén. Naopak může docházet k ohrožujícímu působení v doménách k opatřením změněným, kdy nemusí být nejlepším řešením. V tom je nebezpečnost hybridního působení. Vznikají nové hrozby, kterým se musíme přizpůsobit a najít nová potřebná řešení k ochraně a obranně proti jejich působení.

6 DISKUZE

Bakalářská práce se zabývá tématem Hybridních hrozeb v ČR a schopností čelení bezpečnostního systému ČR ohrožení hybridními hrozbami. Výsledkem práce je definovat potřebné schopnosti moderního státu pro boj proti hybridním hrozbám.

Část přehled současného stavu se zabývá působením a postavením hybridních hrozeb vzhledem k dynamickým změnám dnešní doby plné moderních technologií a neustálého technologického a informačního vývoje.

V této teoretické části je udána historie hybridních hrozeb a válek, jejich vývoj, použití a vliv. Je zde vysvětleno, co je válka, hybridní válka, hybridní hrozba a bezpečnost. U daných pojmů jsou udány definice, popis a příklady. Dále jsou tu uvedeny bezpečnostní struktury a prvky, které jsou aktivními činiteli proti působení hybridních hrozeb. U každého je představení a náplň činnosti.

V praktické části byla vytvořena Tabulka 1 - Zařazení vybraných opatření do sfér DIMEFIL. Za pomoci této tabulky bylo analyzováno pět konkrétních opatření, které pomáhají čelit hybridnímu působení. Pro zjednodušení pochopení tabulky pro nezaujatého čtenáře bylo použito barev, které jsou ztotožněním pro vnímání pozitivního nebo negativního sdělení, tedy zelena, jako „ANO“ a červená, jako „NE“.

Na základě teoretické části a výsledků z části praktické zde navrhnu ke každému z pěti analyzovaných opatření (činnost zpravodajských služeb, informovanost obyvatelstva, kybernetická bezpečnost, mezinárodní smlouvy a dohody, akceschopné ozbrojené síly) několik návrhů. Tyto návrhy by měli vést ke zlepšení vybraných opatření, a tím pádem k jejich efektivnějšímu použití, což ještě více eliminuje možné hrozby nevyžádaných aktivit v doménách DIMEFIL. Opatření jsou posuzována obecně, a je možné, že činnost konkrétních hybridních hrozeb by výsledky v působení na různé domény mohly být odlišné. Pro tuto práci vycházíme z části praktické, která nám definovala rámec působnosti našich opatření

Činnost zpravodajských služeb byla zastoupena ve čtyřech ze sedmi domén spektra DIMEFIL. Tento fakt, však neznamená, že v případě konkrétních hrozeb na určitý cíl zájmu, nemohou působit i v jiných dimenzích moci.

Zpravodajské služby zastávají v rámci zajišťování bezpečnostních zájmů ČR jednu z hlavních funkcí. Zpravodajská činnost je nepostradatelná pro dnešní technologické prostředí a chod moderního státu. Zpravodajské služby získávají informace, které nejsou z běžných médií a veřejných zdrojů dostupné. Zajišťují vojenskou i civilní činnost. Výstupem jejich aktivit je detekce možné trestné činnosti, terorismu, špionáže a podobných negativních působení. Jejich schopnost detekce je na vysoké úrovni.

V rámci návrhu ke zlepšení, nebo minimálně udržení nastavené úrovně, těchto služeb se dle zjištěných skutečností určily zejména tyto tři body. Prvním bodem je reagovat pružně na změny v prostředí, které se mění dynamicky. Nezaspat v legislativním rámci. Obnovovat a vyvíjet dokumenty, ze kterých plynou jejich povinnosti. Zde se jedná zejména o Bezpečnostní strategii ČR a dále konkrétní zákony upravující činnost zpravodajských služeb.

Druhým bodem je budování kolektivní bezpečnosti v rámci EU a NATO, protože čelením společnými silami a použitím více prostředků, budeme my i naši partneři silnější a v rámci ochrany více v bezpečí.

A posledním třetím bodem je důkladná vnitřní kontrola zpravodajských služeb. Kontrolní orgán pro zpravodajské služby sice už vláda ustanovila, ale neřeší, v jakém rozsahu a jakou činnost provádět. Proto by bylo dobré do budoucna jasně stanovit cíle kontrol. Na základě kontrol může být například zamezeno úniku dat nekompetentním personálem nebo naopak vnášení dezinformací infiltrované osoby.

V předcházejících podkapitolách jsme se dozvěděli, jak velkým přínosem je činnost zpravodajských služeb. Avšak jako ve všem, lze vždy něco málo změnit, aby se systém zdokonalil. Zpravodajské služby svou práci odvádějí svědomitě a na vysoké úrovni a nemohou si dovolit nějaké větší chyby, které by nám dali zřetelně najevo větší nedostatky.

Informovanost obyvatelstva se objevila u tří ze sedmi domén spektra DIMEFIL. Jak je v práci několikrát zmíněno, informovanost veřejnosti je podstatná pro jejich rozhodování. Společnost a větší skupiny stejně smýšlejících jedinců lehčeji sugerují názor lehce ovlivnitelným osobám. Z důvodu početnosti osob zastávajících totožný názor je jejich idea okolím více vnímána a její sdělení má silnější význam. Pokud se tato sdělení zakládají na špatně pochopených nebo lživých informacích je těžké rozeznat, kde je původ informace a těžko se s touto skutečností bojuje. Šířit dezinformace nebo s nimi následně manipulovat prostřednictvím podstrčení jiným skupinám, které si ho vysvětlí po svém je v dnešní době poměrně snadné. Čím větší společenství, tím je těžší vyvracet jejich hromadný názor. V rámci osvěty fungují v ČR programy řízené zpravodajskými službami. Tyto vzdělávací aktivity se konají jak pro širokou veřejnost na volně přístupných místech, tak ve firmách a institucích pro své zaměstnance (ať v obecné tématice nebo ke konkrétní pracovní náplni), nebo ve vzdělávacích zařízeních (buď již v rámci začlenění do výuky nebo plánovaných pravidelných přednášek).

Do opatření a návrhů, které by mohly zefektivnit práci obyvatelstva s informacemi, jsou pravidelná či častější školení a vzdělávací aktivity v oblasti zacházení s informacemi a jejich pochopení (tyto aktivity již v některých institucích probíhají v rámci bezpečnosti práce, ale je to jen zlomek institucí a firem). Dále pořádání osvětových kampaní a různých kurzů, kde se uživatel naučí základy k ověřování původu zpráv a věrohodnosti těchto zdrojů. Dávat dostatek času nezávislým médiím, neovlivňovaných politickými nebo mocenskými zájmy. Zamezit šíření zjevných dezinformací a přístupu k informacím, které mají potenciál manipulovat s uživateli. Pokud informaci předává například vlivná organizace nebo veřejně známé a oblíbené osoby, tak na jejich projevy reaguje daleko více lidí. Kvůli reputaci těchto subjektů s nimi i daleko více jedinců sympatizuje a souhlasí, a díky tomu se může stát dalším šiřitelem nepravdivých nebo zmanipulovaných zpráv, i když třeba nezáměrně. Dokonce i subjekty, které interpretujeme nemusí dezinformace šířit úmyslně, neboť si neověřili jejich pravost nebo původ. Informovanost obyvatelstva se udržuje pořádek bezpečný chod společenského dění.

Kybernetická bezpečnost je vzhledem ke globálnímu propojení pomocí internetu, sociálních sítí, uživatelských aplikací, firemních a státních elektronický sytému a dalších podobných nástrojů všudypřítomným opatřením, které je v dnešní době možná i nejdůležitějším opatřením proti působení hybridních hrozeb. Není překvapením, že jakákoliv činnost spojená s kybernetickým prostředím potřebuje své zabezpečení. Nové technologie vytvářejí nové hrozby, kde se zdokonalí obránce, tam musí být kreativnější útočník. Na základě toho útočník vylepšuje své schopnosti a vytváří nové, složitější a komplexnější aktivity k docílení svých zájmů. Není potřeba neustále zdůrazňovat nutnost řádně si chránit svá data a mít pod kontrolou svou činnost v kyberprostoru, ale je to fakt, který je dán dobou. V rámci ČR působí hned několik složek (NÚKIB, NBÚ, VeKySIO a jejich týmy), které plní svou funkci obrany a ochrany v kyberprostoru na vysoké úrovni a jejich schopnost reagovat a bránit se, se neustále zlepšuje a vyvíjí. Důležitým dokumentem je Národní strategie kybernetické bezpečnosti ČR.

Pro uživatele je velmi podstatné v rámci opatření, která mají zamezit nežádoucímu působení proti jejich chráněným hodnotám, zapracovat kromě osvěty a vzdělávání na základních bezpečnostních poučkách k zabezpečení přístupu a ochraně informací. Neotvírat nevyžádané e-mailové zprávy, nenavštěvovat neověřené nebo nezabezpečené weby (pokud nás navíc systém na tento web sám upozorní), volit si silná hesla a nenechávat je někde volně k nahlédnutí (nejhorší a častá chyba, lísteček na monitoru). Zabezpečovat přihlášení dvojitým ověřením (otisk, hlas, heslo, kód). Nenechávat otevřené (odheslované) systémy v přítomnosti neznámých osob. Nevyplňovat osobní čísla dokladů, účtů a ostatních důležitých aktiv, pokud neznám důvod tohoto požadavku. Tyto základní principy se vštěpují všem uživatelům, většinou již při prvotním kontaktu s technologiemi a prostředky pracujícími v kybernetickém prostředí. A pro úplné laiky, když si nejsem opravdu ničím jistý, radši se někoho zeptám, než abych poté řešil následky. Škody způsobené nevyžádaným nakládáním s informacemi a údaji, jiných osob, skupin či subjektů jsou neadekvátně většího rozsahu, než jakékoliv náklady a věnované prostředky na řádné zabezpečení.

Pro orgány působící v ochranně kybernetického prostředí je nezbytné provádět nepřetržitý monitoring možných hrozeb, neustálý vývoj a modernizaci z důvodu vyspělejších hrozeb a aktivit. Pokračovat v národní a nadnárodní spolupráci v čelení hrozbám.

Mezinárodní smlouvy a dohody působily v rámci opatření v pěti ze sedmi domén spektra DIMEFIL. Mezinárodní smlouvy a dohody mohou být uzavřeny na jakýkoliv produkt nebo službu požadovanou smluvními stranami, takže se zde objevuje velký rozsah sfér, na které se smlouvy vážou.

Opatřením v tomto případě je uzavírat smlouvy, které jsou pro nás výhodné nebo výhodné oboustranně. Uzavírat smlouvy, které jsou vymahatelné a splnitelné. V rámci partnerských státu udržovat přátelské vztahy a diplomatické styky, k udržení stávajících smluv a zisku nových možných kontraktů. Budovat si stabilní renomé v rámci aliančních partnerů. Díky vyšší reputaci budeme pro stávající, ale i potenciální mezinárodní partnery lukrativnějším společníkem. Značka se lépe prodává, avšak chyby jdou lépe vidět a nikdo je nezapomene.

Z naší strany, pak plnění závazků a povinnosti, které jsme na sebe v rámci dohod a spolupráce dobrovolně vzali. Plnění těchto povinností nejen posiluje důvěru a politické styky státu v rámci mezinárodních aktivit, ale ukazuje i morálku národa, která dále zvedá reputaci ČR.

Akceschopné ozbrojené síly se svou působností objevily ve třech ze sedmi domén spektra DIMEFIL. Neznamená to, že by ozbrojené síly nebyli ve zbytku domén kompetentní. Opět záleží na konkrétní hrozbě, která bude působit specificky a jejímu čelení bude zapotřebí rozdílných činností.

K jejich zapojení, pokud se nejedná a ozbrojený konflikt nebo cizí agresi vůči suverenitě státu, bývá zapotřebí mimořádných událostí většího rozsahu (v těchto případech se zapojují jako ostatní složky integrovaného záchranného systému). V rámci udržení obranyschopnosti státu je samozřejmě AČR primárním činitelem.

Návrhy a opatření k udržení akceschopných ozbrojených sil vyplývají ze základních potřeb, které má AČR, Hradní stráž a kancelář prezidenta republiky. Pro zabezpečení kvalitních a funkčních struktur ozbrojených sil musí být tyto potřeby zajištěny. Jde o personální naplněnost, materiální vybavenost (nejen k pokrytí a zabezpečení současných kapacit, ale i množstvím odpovídajících rezerv a zásob pro řešení mimořádných událostí a hrozeb) a technologickou vyspělost (nejen mít nové technologie, ale umět je řádně využít a ovládat rozsah možností, které nám skýtají).

K zvýšení naplněnosti ozbrojených sil slouží v dnešní době vícero prostředků. V ČR jsou Krajská vojenská velitelství v rámci, kterých fungují rekrutační centra. Jejich zaměstnanci jezdí v rámci krajů do škol, na veřejné akce nebo organizují vlastní akce, kde přibližují činnost ozbrojených sil zájemcům. Dále se vysílají různé informační a náborové spoty, zejména v komerčních rádiích (vlastní zkušenost) a v současné době se zájemci obracejí a informují přes sociální sítě. V posledních dvou letech se úroveň propagace a prezentace ozbrojených sil v rámci těchto sítí velmi kvalitativně zvedla. Díky tomu oslovuje celou řadu nových adeptů a rozšiřuje pozitivně povědomí a ozbrojených silách. Správná reputace také přivádí nové zájemce. Úroveň naplněnosti stavu je potřeba kontrolovat i zevnitř, tedy odchodem stávajících VZP. K tomu, aby VZP neměli důvod odcházet ze služebního poměru je vhodné je morálně a hodnotně motivovat, VZP. V rámci morálního přesvědčení, by měl voják vědět, že hájí důležité a klíčové hodnoty, jejichž význam by mu měl být pozitivně vštěpován (jedním z hlavních důvodů ke vstupu do ozbrojených sil, je touha bránit vlast a chránit obyvatelstvo ČR, je škoda, že tato původní motivace se u většiny VZP časem vytrácí). Motivace může probíhat i finančně (odměny, náborový příspěvek, proplácení některých nákladů aj.) věcně (různé dary za odvedenou činnost a odsloužené roky ve službě) či kariérně (povýšením, formou výběrových kurzů, dobrovolnou změnou pozice).

Dalším opatřením je nepřetržitý profesionální růst, což je míněno jako příprava, vzdělávání a výcvik. Být VZP je profese, proto se jako profesionál musí každý příslušník neustále zdokonalovat a vzdělávat ve všech oblastech své působnosti. V ovládání zbraní (zlepšením manipulace a znalostí zbraní déle

užívaných i učením se užívání zbraní nových), správné a funkční použití osobního vybavení (kompletace různých součástek výstroje, správné využití konkrétních pomůcek ve vhodném prostředí atd.) V rámci zařazení poté úkony k dokonalému ovládání konkrétní techniky (kolová vozidla, pásová vozidla, vrtulníky a letadla). zabezpečení je potřeba neustále držet krok s nepřítelem a modernizovat výstroj a výzbroj. Ať výstroj a vybavení jedince, tak techniku (pozemní, vzdušnou, obojživelnou).

Pokud není vyložené nutná obměna materiálu (nesplňuje již svou funkci nebo dochází k plošné modernizaci výstroje), tak se nemusí materiální kapacity řešit pouze nákupem, ale i řádnou údržbou. Jendou ze základních povinností voják je starat se o svěřený majetek, provádět jeho řádnou údržbu a předcházet předčasnému poškození. V čím lepší kvalitě je materiál předáván, tím déle vydrží. Samozřejmě nákupy potřebného materiálu jsou stále dominantní složkou k naplnění či doplnění daného vybavení.

Určitě velmi důležitou součástí těchto opatření musí být technická vybavenost. Mít na stavech a disponovat potřebným počtem vojenských vozidel a vzdušných prostředků. Mít tuto techniku v provozuschopném a plně funkčním stavu. V rámci modernizace techniku obměňovat nebo vylepšovat určité komponenty na dané technice. Modernizace je vyžadována vlivem pokroku a vývoje nových útočných i obranných sytému a prostředků.

K tomu všemu je zapotřebí mít dostatek financí. V rámci závazku NATO se všechny členské země zavázali přispívat/dávat na armádu dvě procenta HDP. Průměrem NATO je 1,7 procenta HDP a ČR dává zhruba 1,35 procenta HDP. Již teď je známo, že stanovený plán na 2 procenta HDP v roce 2024 nebude splněn.

Během tvorby této práce jsem si rozšířil povědomí o působení hybridních hrozeb a bezpečnostních systémech sloužících k čelení těmto hrozbám.

7 ZÁVĚR

Hybridní hrozby, kterým je vystavována ČR působí zejména v oblastech hodnot a idejí zakotvených ve společnosti a v ústavním uspořádání státu. Pomocí těchto hodnot je působeno na důležité struktury státu (média, ozbrojené síly a složky, politické struktury a jiné). Cílem těchto ofenzivních aktivit je narušení stability vnitřního prostředí a demoralizace společnosti.

Hybridní hrozby působí pomocí konvenčních i nekonvenčních prostředků. Dochází k prolínání vlivu jednotlivých sfér moci, ve kterých se hybridní hrozby koordinují. Neustále zlepšování technologií a modernizace elektronických systémů vede ke zlepšování metod hybridního působení. Díky moderním trendům se rapidně zvětšila rychlost a rozsah aktivit hybridního působení. Především digitální systémy a jejich snadná dostupnost zvyšují riziko zneužití osobních informací uchovaných v kybernetickém prostoru. Terčem útoku se dnes může stát úplně každý, kdo splňuje zájmy útočníka. Hybridním hrozbám lze čelit jen za pomoci komplexní celospolečenské spolupráci. V rámci prevence a připravenosti je potřeba neustále vzdělávat a školit státní aparát i obyvatelstvo ohledně chování v kybernetickém prostředí a internetové gramotnosti. Podstatnou činností pro chod moderní státu je schopnost jeho obyvatel v oblasti zacházení a manipulace s informacemi. Je velmi důležité, aby občané uměli ověřovat informace, které přebírají z internetových zdrojů.

Vzhledem k informacím a údajům v této práci mohu konstatovat, že schopnosti prvků a schopnost bezpečnostního systému ČR v oblasti detekce a čelení hybridním hrozbám je na kvalitní úrovni a všechny dotčené subjekty svou činnost plní, jak nejlépe mohou a využívají všech dostupných a možných prostředků k co nejefektivnějšímu vedení svých činností.

Slovo hybrid, potažmo hybridní, je za mou osobou zcela správně použito pro činnost, která působí prostřednictvím těchto hrozeb. Vzájemným působením více specifických hrozeb na konkrétní cílové zájmy, vytváří dle situace nové a složitější hrozby a rizika.

8 SEZNAM POUŽITÝCH ZKRATEK

AČR	Armáda České republiky
BIS	Bezpečnostní informační služba
CERT	Computer Emergency Response Team (Skupina pro reakci na počítačový stav nouze)
CIMIC	Civil-Military-Interaction (Civilní-Vojenská-Interakce)
CSIRT	Computer Security Incident Response Team (Skupina pro reakci na počítačové bezpečnostní události)
CTHH	Centrum proti terorismu a hybridním hrozbám
ČR	Česká republika
DIMEFIL	Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal (diplomacie/politika, informace, ozbrojené síly, ekonomika, finančnictví, zpravodajství, veřejný pořádek a právní stát)
EU	Evropská unie
KFOR	Kosovo Force (Síly na území Kosova)
MO	Ministerstvo obrany
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSN	Organizace spojených národů
PSYOPS	Psychologické operace
RF	Ruská federace
UA	Ukrajina
USA	Spojené státy americké
ÚZSI	Úřadu pro zahraniční styky a informace
VeKySIO	Velitelství kybernetických sil a informačních operací
VZ	Vojenské zpravodajství
VZP	Voják z povolání

9 SEZNAM POUŽITÉ LITERATURY

[1] Deník.cz. Věda. *Hybridní hrozby jsou s námi od nepaměti. Znali je už ve starověku* [online] 16.4.2022. Citováno dne 6.5.2022. Dostupné z: https://www.denik.cz/veda/hybridni-hrozby-strach-valka-cina-rusko-amerika.html

[2] ŠTALMACH, Pavel. Hybridní hrozby – včera, dnes a zítra – pohled z Prahy. *Vojenské rozhledy.* 2018, 26 (4) ISSN 1210-3292 (tisk), 2336-2995 [on-line]. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-prostredi/hybridni-hrozby

[3] STOJAR, Richard. Vývoj a proměna konceptu hybridní války. *Vojenské rozhledy*. 2017, 26 (2), 44-55. DOI: 10.3849/2336-2995.26.2017.02.044-055. ISSN 1210-3292 (print), 2336-2995 (on-line). Dostupné z: www.vojenskerozhledy.cz

[4] CLAUSEWITZ, Carl von. O válce. Přeložil Zbyněk SEKAL. Praha: Academia, 2008. Europa (Academia). ISBN 978-80-200-1598-3.

[5] Ministerstvo vnitra České republiky. *Válečný stav* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.mvcr.cz/clanek/valecny-stav.aspx

[6] SUNZI. Umění války: The art of war. 2. vyd. Přeložil Radim PEKÁREK. Brno: B4U, 2014. ISBN 978-80-87222-35-5.

[7] ŘEHKA, Karel. Informační válka. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2.

[8] Praha: Asociace pro mezinárodní otázky, 2015. *Hybrid threats* [online]. Citováno dne 6.5.2022. Dostupné z: http://www.amo.cz/cs/prazsky-studentsky-summit/hybrid-war/.

[9] KŘÍŽ, Zdeněk, Zdeněk KŘÍŽ, Zinaida SHEVCHUK a Peter ŠTEVKOV. Hybrid warfare: A new phenomenon in Europe's security environment. Praha: Jagello 2000 for NATO Information Centre in Prague, 2015. ISBN 978-80-904850-3-7.

[10] ZŮNA, Pavel, Kritický pohled na koncept hybridních válek, Vojenské rozhledy, 2010, roč. 19 (51), č. 3, s. 33-45, ISSN 1210-3292

[11] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, 2007 [on-line]. Citováno dne 6. 5. 2022. Available at:

https://www.potomacinstitute.org/images/stories/publications/potomac_hybrid war_0108.pdf

[12] MAREK, Jindřich a Josef TUREK. 4. brigáda rychlého nasazen 1994-2014. 2., upravené a rozš řené vydán Praha: Ministerstvo obrany České republiky-Vojenský historický ústav Praha, 2015. ISBN 978-80-7278-662-6.

[13] NATOAKTUAL. *Hybridní hrozby v České republice a jak jim čelit* [online]. © 2016. Citováno dne 6.5.2022. Dostupné z: https://www.natoaktual.cz/analyzy-a-komentare/hybridni-hrozby-v-ceske-republice-a-jak-jim-celit.A161020_164518_na_nazory_m02

[14] Lubom r SVĚTNIČKA. NATOAKTUAL. *Hybridní války dávno známe, přesto je musíme objevit a popsat* [online] 14.7.2015. Citováno dne 6.5.2022. Dostupné z: https://www.natoaktual.cz/analyzy-a-komentare/hybridni-valky-davno-zname-presto-je-musime-objevit-a-popsat.A150714_133516_na_analyzy_m02

[15] Ministerstvo vnitra. *o jsou hybridní hrozby* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

[16] Národn strategie pro čelen hybridn mu působen National strategy for countering hybrid interference. Praha: Ministerstvo obrany České republiky-VHÚ Praha, 2021. ISBN 978-80-7278-827-9.

[17] Obranná strategie České republiky: The defence strategy of the Czech Republic. Praha: Ministerstvo obrany České republiky-VHÚ Praha, 2017. ISBN 978-80-7278-702-9.

[18] Národn strategie kybernetické bezpečnosti České republiky. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2020. Citováno dne 6.5.2022. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[19] Výročn zpráva Bezpečnostn informačn služby za rok 2020 [online]. *Bezpečnostní informační služba České republiky,* 2021. Citováno dne 6.5.2022. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf

[20] Vojenské zpravodajství České republiky. *Výroční zpráva o činnosti Vojenského zpravodajství za rok 2020* [Online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41

[21] KARAFFA, Vladimír, Martin HRINKO a Jaromír ZŮNA. Vybrané kapitoly o bezpečnosti. Praha: CEVRO Institut (vysoká škola), 2022. ISBN 978-80-87125-35-9.

[22] Bezpečnostní strategie České republiky [online]. Ministerstvo zahraničních věcí České republiky, 2015. ISBN 978-80-7441-005-5. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[23] Modul-B: zajišťování obrany státu. Praha: Ministerstvo vnitra, 2020. ISBN 978-80-7616-066-8.

[24] *Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky* [online]. 22. dubna 1998. Citováno dne 6.5.2022. Dostupné z: https://www.zakonyprolidi.cz/cs/1998-110

[25] Vláda České republiky. *Audit národní bezpečnosti 2016* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: www: Audit národní bezpečnosti | Vláda ČR (vlada.cz)

[26] Bezpečnostní informační služba. *O nás* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.bis.cz/o-nas/

[27] Vojenské zpravodajství. *Kdo jsme* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.vzcr.cz/kdo-jsme-35

[28] ÚŘAD PRO ZAHRANIČNÍ STYKY A INFORMACE. *Kdo jsme* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.uzsi.cz/kdo-jsme

[29] Národní bezpečnostní úřad. *O nás* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

[30] Národní úřad pro kybernetickou a informační bezpečnost. *O NÚKIB* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[31] Národní centrum kybernetické bezpečnosti. *Co je NCKB* [online]. 2022. Citováno dne 6.5.2022. Dostupné z: https://www.govcert.cz/cs/

[32] Ministerstvo vnitra České republiky. *Centrum proti terorismu a hybridním hrozbám* [online]. 2022. Citováno dne 6.5.2022. Dostupné z:

https://www.mvcr.cz/cthh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx

[33] Ministerstvo obrany České republiky. *VÝVOJ SKUTEČNÝCH POČTŮ OSOB V RESORTU MO ČR V LETECH 1992–2021* [online]. 17.1.2022. Citováno dne 6.5.2022. Dostupné z: https://mocr.army.cz/scripts/detail.php?id=129653

[34] Armáda České republiky. *VELITELSTVÍ INFORMAČNÍCH A KYBERNETICKÝCH SIL* [online] 7.9.2021. Citováno dne 6.5.2022. Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

[35] HAVLÍK Martin. Jak daleko má svět k dosažení světového míru a proč? *Vojenské rozhledy*. 2020, 29 (3), 072-086. ISSN 1210-3292 (print), 2336-2995 (on-line). Dostupné z: www.vojenskerozhledy.cz.

[36] Čítárny. *Overtonova okna aneb šest kroků od nemyslitelného k uzákoněnému* [online] 15.8.2019. Citováno dne 6.5.2022. Dostupné z: https://www.citarny.cz/knihy-lide/vzdelavani-a-souvislosti/souvislosti/overtonova-okna-aneb-sest-kroku-od-nemyslitelneho-k-uzakonenemu

[37] Armáda České republiky. *Součástí kybernetických sil se stali odborníci na civilně-vojenskou spolupráci a PSYOPS.* [online] 10.1.2020. Citováno dne 6.5.2022. Dostupné z: https://acr.army.cz/informacni-servis/zpravodajstvi/soucasti-kybernetickych-sil-se-stali-odbornici-na-civilne-vojenskou-spolupraci-a-psyops-218494/

[38] E15.cz. Zahraniční *Donbas trpěl ve všech dobách. Pohnutá historie uhelné oblasti* [online] 20.4.2022. Citováno dne 6.5.2022. Dostupné z: https://www.e15.cz/donbas-historie-mapa-ukrajina-rusko

[39] Microsoft. Microsoft support. *Co je to kybernetická bezpečnost?* [online] 2022. Citováno dne 6.5.2022. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-to-kybernetick%C3%A1-bezpe%C4%8Dnost-8b6efd59-41ff-4743-87c8-0850a352a390

[40] *Vyhláška č. 157/1964 Sb. Vyhláška ministra zahraničních věcí o Vídeňské úmluvě o diplomatických stycích*. In: Zákony pro lidi [online] 25.04.1964. Citováno dne 6.5.2022. Dostupné z: https://www.zakonyprolidi.cz/cs/1964-157

[41] NATOAKTUAL. Zpravodajství. *Washingtonská smlouva* [online] 2022. Citováno dne 6.5.2022. Dostupné z: https://www.natoaktual.cz/zpravy/Iwashingtonskasmlouva

[42] Ministerstvo zahraničních věcí České republiky. *Mezinárodní smlouvy* [online] 2022. Citováno dne 6.5.2022. Dostupné z: https://www.mzv.cz/jnp/cz/zahranicni_vztahy/mezinarodni_smlouvy/index.html

[43] Ministerstvo financí České republiky. Legislativa. *Přehled dohod o podpoře a ochraně investic* [online] 10.12.2021. Citováno dne 6.5.2022. Dostupné z: https://www.mfcr.cz/cs/legislativa/dohody-o-podpore-a-ochrane-investic/prehled-dohod-o-podpore-a-ochrane-invest

[44] Národní bezpečnostní úřad. Mezinárodní vztahy. *Mezinárodní smlouvy o výměně a vzájemné ochraně utajovaných informací* [online] 2022. Citováno dne 6.5.2022. Dostupné z: https://www.nbu.cz/cs/mezinarodni-vztahy/941-mezinarodni-smlouvy-o-vymene-a-vzajemne-ochrane-utajovanych-informaci/

10 SEZNAM POUŽITÝCH TABULEK