Univerzita Palackého v Olomouci
Filozofická fakulta
Katedra politologie a evropských studií

Simona Weissbergerová

Role NATO v boji proti kybernetickým útokům na kritickou infrastrukturu České republiky

Role of NATO in the fight against cyber attacks on the critical infrastructure of the Czech Republic

Bakalářská diplomová práce

Vedoucí práce: Mgr. Veronika Krátká Špalková

Olomouc 2023

Prohlašuji, že jsem bakalářskou diplomovou práci na téma *„Role NATO v boji proti kybernetickým útokům na kritickou infrastrukturu České republiky“* vypracovala samostatně na základě uvedených pramenů a literatury.

V Olomouci dne 27. 4. 2023 …….

Simona Weissbergerová

Poděkování

Na tomto místě bych ráda poděkovala vedoucí práce Mgr. Veronice Krátké Špalkové za poskytnutí cenných rad, odborný dohled a trpělivost.

Obsah

Úvod

Bezpečnost České republiky (ČR) by neměla být považována za samozřejmost. Kybernetické útoky jsou jednou z největších hrozeb ve 21. století nejen v ČR, ale i ve světě. Představují významné riziko pro kritickou infrastrukturu, která zahrnuje např. energetický, státní i soukromý sektor, vojenské cíle, zdravotnictví apod. Každý útok může mít významné dopady na bezpečnost obyvatelstva a státu. Útoky se nevyhýbají ani naší zemi a ČR každoročně čelí stovkám kybernetickým útokům, které způsobují nemalé finanční škody. Odborník na kybernetickou bezpečnost Daniel Bagge v rozhovoru pro Novinky.cz (2018) prohlásil: *„NATO kyberprostor zařadilo mezi operační domény, aby vyslalo signál případným oponentům a také aby přimělo členské státy, aby se problému začaly věnovat a přizpůsobily své operační postupy.“* Vzhledem k neustálému pokroku v oblasti high-tech technologií a rostoucí závislosti obyvatel na chytrých zařízeních, roste množství hrozeb a kybernetických útoků, kterým denně běžní občané čelí. Kybernetické útoky se staly nástrojem hybridní války a mají za cíl ochromit kritickou infrastrukturu nebo se dostat k citlivým datům. Stopy po útočnících často vedou za hranice státu, především do zemí jako je Čína, Rusko nebo Severní Korea. Úkolem Severoatlantické aliance (NATO) je zajistit bezpečnost členských zemí prostřednictvím politických a vojenských prostředků. NATO musí být schopné reagovat na nové výzvy v oblasti kybernetiky, jelikož se hackeři neustále v kybernetických útocích zdokonalují. Posílením obrany a bezpečnosti kyberprostoru se vedle vlád, odborných institucí, NATO, začaly věnovat i soukromé firmy. Žádná země nemůže čelit kybernetickým hrozbám sama, proto je důležitá soudržnost a spolupráce v rámci NATO.

Časové vymezení bakalářské práce se pohybuje v letech 2013–2022, jelikož první zpráva o stavu kybernetické bezpečnosti ČR byla vydána teprve v roce 2013.

Bakalářská práce je z hlediska metodologie deskriptivní analýzou s exploračním charakterem. Deskriptivní práce neprodukuje nové teorie, přesto plní důležitou roli v rámci vysvětlujícího výzkumu. Přínosem deskriptivní analýzy je sbírání a shromažďování faktů, které mohou být využity při tvorbě nebo testování hypotéz a teorií. Popis je jedním z možných a legitimních výzkumných cílů, jemuž se v této práci budu věnovat (Beneš & Císař, 2020).

Bakalářská práce hledá odpovědi na následující výzkumné otázky:

„*Jakou pomoc poskytuje NATO členským zemím, na základě oficiálních dokumentů, v boji proti kybernetickým útokům?“*

„Jakým způsobem NATO pomáhá členským zemím při budování kapacit pro kybernetickou bezpečnost?“

„Disponuje NATO orgány, které se zabývají kybernetickými hrozbami a kybernetickými útoky na členské země?“

„Které české orgány se zabývají kybernetickými hrozbami a kybernetickými útoky na kritickou infrastrukturu?“

Práce vychází z teorie o internacionalismu. Počátky této teorie sahají do 19. století, kdy v západním demokratickém světě funguje jako politický koncept, jehož cílem je nastavit spolupráci mezi národy. Během tohoto období se státy a společnosti modernizovaly, stávaly se mocnějšími a rozšiřovaly své imperiální a ekonomické hranice. Internacionalismus podporuje a prosazuje mezinárodní instituce jako je např. NATO. V bakalářské práci je teorie aplikovaná na příkladu NATO, která pomáhá zemím budovat kapacity v oblasti kybernetické obrany a poukazuje na významnost spolupráce mezi členy, Výsledkem spolupráce je, že jsou země schopny ustát kybernetické útoky. Teorie liberálního internacionalismu řeší, jak nejlépe organizovat a reformovat mezinárodní systém. Obecně platí, že liberální internacionalisté považují násilí za politiku poslední instance, obhajují diplomacii a multilateralismus jako nejvhodnější strategie (Deines, 2023).

Cílem bakalářské práce je najít odpovědi na výzkumné otázky, provedení průzkumu stavu kybernetické obrany ČR v kontextu členství v NATO. V neposlední řadě je cílem prozkoumat role NATO v boji proti kybernetickým útokům na kritickou infrastrukturu.

Práce je rozdělena do osmi kapitol, které mají poskytnou informace o tématu a odpovědět na stanovené výzkumné otázky. První kapitola popisuje teorii internacionalismu. Druhá kapitola se věnuje speciálním poradním orgánům NATO, které se podílejí na kybernetické obraně členských zemí. Třetí kapitola popisuje české orgány zabývající se kybernetickými útoky a kybernetickou bezpečností. Čtvrtá kapitola popisuje Národní bezpečnostní strategii o kybernetické bezpečnosti ČR, jež představuje cíle, kterých by ČR měla dosáhnout. Pátá kapitola popisuje typy národních i mezinárodních kybernetických cvičení. Šestá kapitola se zabývá kybernetickými útoky, kterým ČR čelila v letech 2013–2022. Sedmá kapitola analyzuje role NATO v boji proti kybernetickým útokům. Osmá kapitola představuje Strategii kybernetické obrany ČR, která stanovuje cíle, kterých by ČR měla dosáhnout i s ohledem na členství v NATO. Za poslední kapitolou následuje závěr, který mimo jiné nabízí odpovědi na výzkumné otázky.

Největším limitem práce byl nedostatek odborné literatury, která by pokrývala téma kybernetických útoků na kritickou infrastrukturu ČR a role NATO v boji proti kybernetickým útokům. Primárním zdrojem informací byly oficiální webové stránky NATO, webové stránky

institucí zabývajících se kybernetickou bezpečností a články českých i zahraničních zpravodajských portálů, jenž poskytovaly nejaktuálnější informace.

Informace, které blíže specifikují jednotlivé orgány NATO, byly taktéž nedostatečné pro zpracování kapitoly *„Orgány NATO podílející se na kybernetické obraně členských zemí.“*. Z tohoto důvodu jsou nezbytné poznatky čerpány z oficiálních webových stránek jednotlivých institucí. Podobná situace nastala také při psaní kapitoly o českých orgánech, které se zabývají kybernetickou bezpečností. I zde bylo čerpáno z oficiálních stránek institucí, jelikož i tato oblast ještě není dostatečně zpracována odbornou literaturou.

Nejvíce přínosným zdrojem informací, který se zabýval tématem kybernetických útoků na kritickou infrastrukturu ČR v letech 2013–2022, byly zprávy o stavu kybernetické bezpečnosti, které od roku 2013 každoročně vydává Národní úřad pro kybernetickou a informační bezpečnost. Tyto zprávy představují jediný souhrnný popis stavu české kybernetické bezpečnosti v těchto letech. Zprávy podrobně popisují počty a typy kybernetických útoků, které zasáhly kybernetický prostor ČR. Zprávy informují také o cvičeních, kterých se ČR zúčastnila.

Národní strategie kybernetické bezpečnosti ČR popisuje hlavní principy, na kterých stojí kybernetická bezpečnost České republiky, definuje její budoucí strategické směřování v oblasti kybernetické bezpečnosti a popisuje základní vize v oblasti kybernetické bezpečnosti. Strategie kybernetické obrany ČR stanovuje podmínky pro zajištění obrany státu v kybernetickém prostoru. Dokument definuje základní vizi a cíle pro plánovaný vývoj kybernetické obrany v jednotlivých oblastech. Bez těchto dvou dokumentů by nebylo možné nastínit cíle a vize v oblasti kybernetické bezpečnosti, kterých by ČR chtěla dosáhnout.

Vhled do vývoje přístupu ke kybernetice NATO přinesl článek *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*, který poskytl informace k summitu NATO ve Varšavě z roku 2016, který byl významný z hlediska uznání kybernetického prostoru jako další operační domény NATO. Zmiňuje také summit NATO v Bruselu v roce 2021, na kterém byla schválena nová komplexní politika kybernetické obrany.

Důležitým zdrojem byla česká kniha *„Kybernetická bezpečnost“*, díky které jsem se do dané problematiky mohla hlouběji ponořit. V této publikaci lze nalézt potřebné informace o samotných útocích, kritické infrastruktuře a samotné kybernetické bezpečnosti.

1. Teorie internacionalismu

V knize *„The logic of internationalism: Coercion and accommodation*“, jejímž autorem je Kjell Goldmann, je internacionalismus popisován jako soubor názorů, které tvrdí, že pokud bude mezi státy existovat a dominovat právo, fungovat organizace, budou probíhat výměny a komunikace, dojde k posílení míru a bezpečnosti. Stejný výklad teorie používal Hedley Bull, když rozlišoval mezi Hobbesovým realismem, Kantovým universalismem a Grotiovým internacionalismem. Existují i jiné způsoby použití tohoto termínu. Hitler i Lenin byli internacionalisté, ale ne ve smyslu budování institucí a spolupráce v zájmu míru a bezpečnosti. Hitler měl globální ambice a Lenin prosazoval světovou revoluci. Kořeny internacionalismu ve 20. století utváří dvě tradice: dlouhá historie návrhů na vznik mezinárodních organizaci a klasický liberalismus s vírou v benefity volného obchodu. Součástí teorie je tvrzení, že volný obchod je mnohem výhodnější než válka, protože přispívá nejen k materiálnímu blahobytu národů, ale také k intelektuálnímu a morálnímu pokroku lidstva. Volný obchod by posílil mírové vazby mezi národy a pacifického ducha mezi lidmi. Svoboda obchodu by podstatně snížila riziko války, nebo je dokonce zcela vyloučila. Richard Cobden byl zastáncem ekonomické analýzy a volného obchodu, který má zabránit mezinárodním konfliktům. Volný obchod by spojoval všechny národy vzájemnou výměnou a byl by synonymem všeobecného souladu. Volný obchod by učinil válku mezi národy nemyslitelnou. Každý obchod a každá továrna by se staly centrem diplomatického systému usilujícího o mír. Již v rané literatuře se objevily čtyři důvody, proč lze očekávat, že mezinárodní organizace přinesou mír. První důvod byl ten, že by se pachatelé konfliktu museli potýkat s vojenskými nebo hospodářskými sankcemi nebo s odsouzením ze strany veřejného mínění. Druhý důvod zahrnoval organizace, které by přispěly k posílení mezinárodního práva. Třetí důvod pojednává o zajištění institucionalizovaného postupů pro řešení konfliktů – arbitráž, soudní řízení, racionální diskuse apod. Čtvrtý důvod byl ten, že po založení organizace by její členové měli zájem na jejím udržením (Goldmann, 2002).

Britský politolog David Mitrany přišel s teorii míru přenesením praktických funkcí státu na instituce na mezinárodní úrovni. Mezinárodní rozdělení mělo být překryto sítí mezistátních agentur. Měl vzniknout mezinárodní systém sociálního zabezpečení, jehož výsledkem by bylo přenesení vazby z národní na mezinárodní úroveň (Goldmann, 2002).

Nejvlivnějším z klasických mírových plánů byl pravděpodobně spis Immanuela Kanta *„Zum ewigen Frieden“* z roku 1795. Kant si představoval evropskou konfederaci, která by tvořila jádro státu národů a zabránila by válce (Goldmann, 2002).

V bakalářské práci je aplikovaná teorie internacionalismu. Z popisu teorie vyplývá, že je důležitá spolupráce mezi zeměmi, jelikož pro všechny účastnící se strany je vzájemná kooperace výhodná. Jako praktický příklad, teorie internacionalismu, bakalářská práce uvádí spolupráci mezi členy NATO, kteří společně čelí kybernetickým hrozbám. Země chtějí být připravené na kybernetické útoky, aby dokázaly ochránit nejen sebe, ale i své alianční partnery. NATO svým členům poskytuje možnost se účastnit školení a cvičení zaměřených na kybernetickou obranu. Článek pět Severoatlantické smlouvy poskytuje svým členům záruku pomoci v případě napadení. NATO taktéž disponuje orgány, které jsou připravené nabídnout pomoc kterékoli členské zemi. Díky takto rozvinuté spolupráci mezi zeměmi nedochází k válečným konfliktům mezi členy, a naopak je udržován mír a členové NATO společně čelí kybernetickým útokům a jiným hrozbám.

2. Orgány NATO podílející se na kybernetické obraně členských zemí

V dnešní době, která je na technologiích závislá, musí NATO každý den čelit protivníkům – i z řad nestátních aktérů, kteří se pokouší skrze kybernetické útoky zastrašit a destabilizovat členské státy NATO. NATO uznalo kybernetický prostor[1] jako svou pátou dimenzi. Vedle země, vzduchu, vody a vesmíru přibyla nová operační oblast – kybernetický prostor. V reakci na kybernetické hrozby, NATO přijalo politiky, akční plány, zřídilo výbory, agentury a operační střediska za účelem integrace kybernetické oblasti. Přístup NATO ke kybernetické obraně se za posledních 15 let vyvíjel. Došlo k de facto uznání, že kybernetický útok může způsobit škody srovnatelné s ozbrojeným útokem (Marrone & Sabatino, 2021).

2.1. Severoatlantická rada

Severoatlantická rada je hlavním a nejvyšším politickým orgánem z celé struktury NATO. Každá členská země má v Radě svého zástupce. Zástupci vedou diskuse o vojenských či politických tématech. Zabývají se otázkami, které mohou ovlivnit bezpečnost a mír členských zemí a neobejdou se bez kolektivního rozhodnutí. Severoatlantická rada byla založena na základě Severoatlantické smlouvy a Článku devět. Rada disponuje rozhodovacími pravomocemi v politických a vojenských záležitostech. Rozhodnutí se přijímají jednomyslně, takže musí dojít ke shodě mezi všemi zástupci a následně ke svým rozhodnutím vydává prohlášení (NATO, 2022).

Ve věcech kybernetické obrany spolupracuje Severoatlantické rada s Výborem pro kybernetickou obranu[2]. Výbor je podřízen Severoatlantické radě a zabývá se politikou kybernetické obrany a politickým řízením (CCDCOE, n.d.).

Zřízení Výboru přispělo k vysílání spojeneckých expertů na kybernetiku do sídla NATO. Došlo tím ke zlepšení spojení mezi sídlem NATO a národními centry, jako je Kybernetické velení[3], Národní bezpečnostní agentura USA[4] a Government Communications Headquarters (GCHQ)[5] ve Spojeném království. Výbor má odpovědnost za sledování implementace Akčního plánu NATO pro kybernetickou obranu[6] a aktualizaci celkové politiky. Rada pro řízení kybernetické obrany sdružuje aktéry, kteří vyhodnocují a reagují na kybernetické útoky a jiné

[1] Kybernetický prostor je virtuální prostředí, ve kterém jsou digitalizované informace uloženy nebo sdělovány prostřednictvím informačních systémů a sítí (Hunker, 2010).
[2] Cyber Defence Committee – CDC
[3] Cyber Command
[4] The National Security Agency (NSA)
[5] Britská vládní zpravodajská a špionážní organizace.
[6] NATO's Cyber Defence Action Plan

incidenty, monitorují hrozby a zajišťují včasné varování. Všechny tyto aktivity pomáhají členským státům v oblasti kybernetické obrany (Shea, 2017).

2.2. Rada pro řízení kybernetické obrany (CDMB)

Rada pro řízení kybernetické obrany působí pod záštitou Emerging Security Challenges Division (ESCD). Skládá se ze zástupců všech hlavních aktérů kybernetické bezpečnosti v rámci NATO – Velitelství spojeneckých sil pro operace, Velitelství spojeneckých sil pro transformaci a agentury NATO. CDMB provádí strategické plánování a výkonné řízení týkající se sítí NATO a podepisuje memoranda o porozumění s členskými státy za účelem usnadnění výměny informací a koordinace pomoci (CCDCOE, n.d.).

2.3. Centrum excelence NATO pro kybernetickou obranu (CCDCOE)

Estonsko bylo hlavním iniciátorem založení CCDCOE[7] spolu se Slovenskem, Německem, Itálií, Španělskem, Litvou a Lotyšskem. Centrum bylo založeno 14. května 2008. Ve stejném roce Severoatlantická rada rozhodla o udělení plné akreditace a statutu Mezinárodní vojenské organizace. Estonsko vstoupilo do NATO v roce 2004 a v tomtéž roce navrhlo koncepci CCDCOE, která byla schválena vrchním velitelem spojeneckých sil pro transformaci v roce 2006. První politicky motivovaný kybernetický útok byl veden proti Estonsku a upozornil ostatní státy na rostoucí význam potenciálních hrozeb v oblasti kybernetiky (CCDCOE, n.d.). Vše začalo v dubnu 2007, kdy bylo rozhodnuto o odstranění sochy rudoarmějce z centra města Tallinnu. Po přemístění bronzového vojáka, spolu s ostatky vojáků na vojenský hřbitov, došlo k pobouření Rusů. Pro ně byl bronzový voják nenáviděným symbolem zvěrstev za Stalina. V Tallinnu se tak začal bouřit dav sestávající se z Estonců a mnoha neintegrovaných Rusů. Několikadenní pozdvižení, které následovalo, mělo za následek smrt jedné osoby, zranění stovky dalších a více než tisíc zadržených. Následně došlo ke kybernetickému útoku, který byl zaměřen na kritickou ekonomickou a politickou infrastrukturu Estonska a v některých případech trval i týdny (Jiri, & Valenta, 2018). Útoky pocházely z ruských IP adres, pokyny k útoku byly v ruském jazyce a Moskva ignorovala výzvy Estonska o pomoc. Neexistuje však žádný konkrétní důkaz, že tyto útoky skutečně provedla ruská vláda (McGuinness, 2017). Tento útok upozornil země na rostoucí význam potenciálních hrozeb v oblasti kybernetiky (CCDCOE, n.d.).

[7] CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence

K aktivitám CCDCOE patří konference o kybernetické bezpečnosti. První konference se konala v roce 2009 a hlavními tématy byly právní a technologické aspekty a výzkum kybernetických konfliktů. CCDCOE každoročně pořádá Mezinárodní konference o kybernetických konfliktech (CyCon). CyCon je prestižní akcí zaměřenou na budování komunity kybernetické obrany. Každoročně se na CyConu schází odborníci a osoby s rozhodovacími pravomocemi, aby společně řešili aktuální výzvy v oblasti kyberbezpečnosti (CyCon, n.d.).

CCDCOE participuje téměř na všech hlavních cvičeních NATO a na dalších národních nebo mezinárodních iniciativách. Mezi cvičeními, které CCDCOE podporuje patří např. Coalition Warrior Interoperability eXercise (CWIX). Jedná se o největší test interoperability NATO. CWIX – jde o cvičení, ve kterém spojenci a partneři NATO procvičují techniku, taktiku a postup pro zlepšení detekce kyberútoků a doby odezvy potřebné k identifikaci a řešení nově vznikajících bezpečnostních hrozeb (International Conference on Cyber Conflict, n.d.).

2.4. NATO Cyberspace Operations Centre (CYOC)[8]

V roce 2023 by mělo být uvedeno do provozu nové Kybernetické operační centrum NATO v belgickém městě Mons. CYOC bude provádět kybernetické operace za účelem podpory vojenských kinetických operací ve fyzické oblasti (Disma, 2019). Nové centrum by mělo být připraveno provádět operace v kybernetickém prostoru, posilovat obranu NATO a koordinovat prostředky k odstrašení prostřednictvím 70členného týmu odborníků. CYOC by mohlo, pro zajištění své obrany, zničit počítačové sítě nebo použít kybernetické zbraně k obraně před nepřátelskými raketami nebo k obraně vzdušného prostorou (Emmott, 2018).

2.5. NATO Computer Incident Response Capability (NCIRC)

Na Pražském summitu NATO v roce 2002 byl přijat Program kybernetické obrany a došlo k rozhodnutí vytvořit NCIRC (Ducaru, 2016). NCIRC má sídlo ve Vrchním velitelství spojeneckých sil v Evropě, které se nachází belgickém městě Mons. K úkolům NCIRC patří chránit sítě NATO. Jednotliví odborníci řeší kybernetické incidenty, poskytují spojencům a členům NATO analýzu jednotlivých kybernetických problémů. NCIRC je součástí Agentury komunikačních a informačních systémů NATO[9], která propojuje informační a komunikační systémy NATO, podporuje operace NATO a brání jeho sítě (NATO, 2021).

[8] Volně česky přeloženo jako Kybernetické operační centrum NATO.
[9] NATO Communications and Information Agency (NCI Agency)

Agentura NCIA byla založena 1. července 2012 a vznikla sloučením organizací NATO C3. Došlo ke sloučení: Agentury NATO pro komunikační a informační systémy[10], Agentury NATO pro konzultace, velení a řízení[11], Agentury NATO pro řízení systému velení a řízení vzdušných sil[12], Službu informačních a komunikačních technologií ústředí NATO[13] a Programovou kancelář NATO pro obranu proti balistickým střelám[14]. Zaměstnává přibližně 3000 civilních a vojenských zaměstnanců, kteří zajišťují nepřetržitou ochranu sítí NATO a bezpečnost pro téměř miliardu občanů (NATO Communications and Information Agency, n.d.).

[10] NATO Communication and Information Systems Services Agency (NCSA)
[11] NATO Consultation, Command and Control Agency (NC3A)
[12] NATO ACCS Management Agency (NACMA)
[13] Information Communications and Technology Management (ICTM)
[14] Active Layered Theatre Ballistic Missile Defence (ALTBMD)

3. Orgány České republiky zabývající se kybernetickými útoky

ČR se intenzivně věnuje obraně kybernetického prostoru a snaží se bojovat proti kyberútokům, které mohou ohrozit kritickou infrastrukturu, ale i zdraví a život občanů. V ČR najdeme několik aktérů, kteří se věnují ochraně a obraně kyberprostoru. K hlavním aktérům patří: Národní úřad pro kybernetickou a informační bezpečnost, Národní centrum kybernetické bezpečnosti, Vojenské zpravodajství, Velitelství kybernetických sil a informačních operací, Národní centrála proti organizovanému zločinu (NÚKIB, 2020a).

Do roku 2007 se kybernetickou bezpečností zabývalo Ministerstvo informatiky. V roce 2007 došlo k jeho zrušení a část ministerstva se sloučila s Ministerstvem vnitra. Tento krok nenaplnil očekávání, jelikož Ministerstvo vnitra nezvládalo plnit závazky v oblasti kybernetické bezpečnosti. Z těchto důvodů byl v roce 2011 ustanoven Národní bezpečností úřad, konkrétně jeho součást – Národní centrum kybernetické bezpečnosti. V roce 2017 zahájil svou činnost Národní úřad pro kybernetickou a informační bezpečnost, který byl novelou zákona vyčleněn z Národního bezpečnostního úřadu (Hrůza, 2015).

V roce 2014 vstoupil v platnost klíčový dokument ČR, a to zákon o kybernetické bezpečnosti, který upravuje práva a povinnosti osob v oblasti kybernetické bezpečnosti. K hlavním cílům zákona patří: *„Stanovit základní úroveň bezpečnostních opatření, zlepšit detekci kybernetických bezpečnostních incidentů, zavést hlášení kybernetických bezpečnostních incidentů, zavést systém opatření k reakci na kybernetické bezpečnostní incidenty a upravit činnost dohledových pracovišť.“* (NÚKIB, n.d.e).

3.1. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

„NÚKIB[15] *je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo.“* (NÚKIB, n.d.f).

NÚKIB je institucí, která státu poskytuje expertízu k zajištění určité nezávislosti na třetích stranách. Hodnotí úroveň bezpečnosti systémů pracujících s utajovanými informacemi a řeší případné bezpečnostní hrozby. Koordinuje výměnu informací, získává informace od partnerů, doporučuje opatření pro řešení problémů a analyzuje data. Poskytuje služby spojené s auditem plnění bezpečnostních standardů dle platných norem. Důležitou součástí je edukace a tréninky

[15] *„NÚKIB vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“* (NÚKIB, n.d.f).

v oblasti kyberbezpečnosti. Zabývá se také monitoringem a analýzou trendů, zpracovává návrhy bezpečnostních strategií a politik v této oblasti. Nedílnou součástí je regulace prostřednictvím identifikace, případně certifikace důležitých informačních a komunikačních systémů, kontrola dodržování zákonných norem a bezpečnostních standardů. NÚKIB by se neobešel bez mezinárodní spolupráce, bez níž by ČR nemohla ovlivňovat tvorbu mezinárodních standardů a politik v rámci v rámci NATO, EU či OSN (NÚKIB, 2020).

3.2. Národní centrum kybernetické bezpečnosti (NCKB)

NCKB je výkonnou sekcí NÚKIB. Sekce NCKB zajišťuje činnost Vládního CERT ČR (GovCERT.CZ), zabývá se prevencí a řešením kybernetických bezpečnostních incidentů u kritické infrastruktury, provozovatelů základní služby a veřejné správy. Spolupracuje s národními i mezinárodními organizacemi, které se podílejí se na zajišťování bezpečnosti kyberprostoru. NCKB je účastníkem i organizátorem kybernetických cvičení. Vyhodnocuje rizika v oblasti kybernetické bezpečnosti a přijímá nápravná a preventivní opatření. Dále zajišťuje i výzkum a vývoj v oblasti kybernetické bezpečnosti. Má na starost komunikační strategii Úřadu v oblasti kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky Úřadu a mnoho dalších aktivit (GovCERT.Cz, n.d.).

Vládní CERT a týmy CSIRT sehrají důležitou roli při ochraně kritické informační infrastruktury a významných informačních systémů. Úlohou těchto týmů je působit jako prvotní zdroj bezpečnostních informací a pomoci pro občany, organizace a orgány státu. Stejně důležitou roli hrají při edukaci v oblasti bezpečnosti na internetu. Po nahlášení kybernetického bezpečnostního incidentu jsou členové vládního týmu připraveni pomoci a poskytnout rady pro další preventivní opatření (NCKB, n.d.b).

3.3. Vojenské zpravodajství (VZ) a Národní centrum kybernetických operací (NCKO)

„Vojenské zpravodajství je jednotnou ozbrojenou zpravodajskou službou České republiky integrující rozvědnou a kontrarozvědnou činnost. Základním úkolem Vojenského zpravodajství je získávat, shromažďovat a vyhodnocovat informace důležité pro obranu České republiky. Vojenské zpravodajství je přímou součástí Ministerstva obrany. V jeho čele stojí ředitel, který je z výkonu své funkce odpovědný ministru obrany.“ (Vojenské zpravodajství, n.d.c). 1. července 2021 nabyla účinnosti novela zákona o VZ zabývající se kyberobranou. *„Zákon vychází z požadavků strategie vytvořené Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a schválené vládou. Nutnost vychází i ze členství*

v *Severoatlantické alianci (NATO), která uznala kybernetický prostor v roce 2016 za operační doménu.“* (Vojenské zpravodajství, n.d.b). VZ se začalo podílet na kybernetické obraně ČR, kvůli riziku konfliktu v kyberprostoru. VZ zřizuje Národní centrum kybernetických operací (NCKO). Úkolem VZ je vytvoření účinného systému obrany v kybernetickém prostoru, aby ČR zvládla zastavit a odvrátit kybernetické útoky, a tím zabezpečit ochranu civilního obyvatelstva a infrastruktury. Výhodou VZ je, že působí nejen v ČR, ale i v zahraničí. Parlament ČR schválil právní úpravu[16], která umožnila VZ podílet se na kybernetické obraně (Vojenské zpravodajství, n.d.a).

K rolím VZ patří řešení nejzávažnějších kybernetických útoků, které pocházející ze zahraničí a ohrožující fungování státu. VZ se podílí na obranných opatřeních, detekuje kybernetický útok a může předat informace k provedení opatření jiné instituci či subjektu nebo přímo zasáhnout (krajní řešení). VZ je kontrolováno vládou, ministrem obrany, sněmovní komisí, Orgánem nezávislé kontroly a Inspektorem. Důležitou součástí je spolupráce se státními institucemi a soukromým sektorem (Vojenské zpravodajství, n.d.b).

NCKO představilo Strategii kybernetické obrany pro období 2018 až 2022. Dokument formuluje základní cíle a vize, které popisují plánovaný vývoj kybernetické obrany v jednotlivých oblastech. Kybernetické pracoviště Vojenského zpravodajství změnilo svůj název z Národního centra kybernetických sil na Národní centrum kybernetických operací (NCKO) (Riethofová, 2018).

3.4. Velitelství kybernetických sil a informačních operací (VeKySIO)

Velitelství informačních a kybernetických sil je strategickým nástrojem, který přispívá k bezpečnosti a obraně ČR. Ve struktuře Armády České republiky spadá do taktické úrovně společně s Pozemními silami, Vzdušnými silami a Velitelstvím teritoria. Velitelství pro operace plánuje, velí a řídí operace sil a prostředků na území ČR i mimo něj. Působí nezávisle, společně nebo v součinnosti s ostatními druhy sil a Vojenským zpravodajstvím. Zakládá si na spolupráci s dalšími prvky kybernetické bezpečnosti a obrany. Může vést operace v kybernetickém prostoru, včetně informačních a psychologických operací, a dále se podílet na civilně-vojenské spolupráci. Disponuje schopností monitorovat, plánovat a řídit operace jak ve prospěch Armády České republiky, tak k podpoře spojeneckých operací. Velitel poskytuje podporu nejvyššímu velení armády v oblasti strategické komunikace (Armáda České republiky, 2021).

[16] Novela zákona č. 289/2005 Sb., o Vojenském zpravodajství

3.5. Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV (NCTEKK SKPV)

Dne 1. srpna 2016 vznikla Národní centrála proti organizovanému zločinu sloučením Útvaru pro odhalování organizovaného zločinu SKPV a Útvaru odhalování korupce a finanční kriminality SKPV. Po zrušení sekce „terorismu a extremismu“ a „kybernetické kriminality“, vznikla nová Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. Národní centrála proti organizovanému zločinu se nyní specializuje na odhalování organizovaného zločinu, finanční kriminality, závažné hospodářské trestné činnosti a korupce (Policie ČR, n.d.a).

Dne 1. ledna 2023 začala fungovat nová Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV a došlo k vytvoření nového samostatného policejního útvaru. Centrála se bude zabývat bojem proti terorismu, extremismu a kyberkriminalitě (Policie ČR, n.d.b). Centrála má celorepublikovou působnost a zaměřuje se na ochranu kritické infrastruktury státu, jako jsou elektrárny nebo státní důležité systémy (Veselá, 2023).

4. Národní strategie kybernetické bezpečnosti ČR 2020–2025

ČR a její společnost jsou kriticky závislí na moderních technologiích a kyberprostoru. ČR je cílem kybernetické špionáže se zaměřením zejména na státní instituce. Roste zájem také o soukromé subjekty, jako jsou malé a střední podniky. Na zajišťování kybernetické bezpečnosti se podílí mnoho subjektů. Za národní bezpečnost, a řízení a funkčnost bezpečnostního systému je odpovědná vláda ČR. K institucím, které zajišťují kybernetickou bezpečnost ČR patří: NÚKIB, Vládní CERT a Národní CERT, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Policie ČR, Úřad pro zahraniční styky a informace, Národní centrála proti organizovanému zločinu SKPV, Bezpečnostní informační služba, Ministerstvo obrany, Vojenské zpravodajství, Generální štáb Armády ČR, Národní centrum kybernetických operací a Velitelství informačních a kybernetických sil. Do systému kybernetické bezpečnosti je zapojeno také Ministerstvo průmyslu a obchodu, potažmo Českého telekomunikačního úřadu. Ministerstvo školství, mládeže a tělovýchovy má vliv na vzdělávání nové generace. Podstatnou roli sehrávají také subjekty ze soukromého sektoru, asociací, akademie, sdružení apod. Sebevědomým, zodpovědným přístupem ke kybernetické bezpečnosti na národní úrovni bude ČR posilovat svou prosperitu, a navíc bude i nadále silným spojencem pro své partnery na mezinárodní úrovni. Pro zajištění účinné obranyschopnosti ČR je důležitý systém detekce kybernetických hrozeb. Sebevědomým a zodpovědným přístupem ke kybernetické bezpečnosti bude ČR posilovat svou prosperitu a zůstane silným spojencem pro své partnery. Zásadní je jednotný přístup států ke kybernetické bezpečnosti a obraně a civilně-vojenská spolupráce v zabezpečování kyberprostoru. Každý jednotlivec, instituce nebo společnost má vlastní úlohu a může přispět k zajišťování kybernetické bezpečnosti. ČR bude pokračovat v navyšování odolnosti strategické informační struktury. ČR potřebuje účinnou strategii komunikace se svými partnery a veřejností, avšak prvně musí plně porozumět informačnímu prostředí. V případě vypuknutí krize nebo konfliktu, bude ČR připravena jednat a v případě potřeby využít diplomatické, politické i silové prostředky vůči agresorovi. ČR se bude snažit dosáhnout co největšího zabezpečení a posilovat svou odolnost v kyberprostoru i v konceptu odstrašování. ČR musí umět čelit budoucím výzvám, umět je identifikovat, analyzovat a vyhodnocovat. Nedílnou součástí je výzkum a inovace v nových technologiích, podpora vzniku nových výzkumných a vývojových center a českého průmyslu v oblasti kyberbezpečnosti. Výzvám kybernetické bezpečnosti můžeme čelit pouze prostřednictvím aktivní mezinárodní spolupráce zahrnující společnou reakci, koordinaci a postup proti kybernetickým hrozbám. ČR bude posilovat svou roli v mezinárodních organizacích (EU, NATO, OBSE, OSN a OECD), na konferencích a fórech. V oblasti moderních technologií patří ČR mezi špičku v Evropě. Díky

tomu dochází k postupné transformaci české společnosti na informační společnost, přestože je stále nedostatečně mediálně gramotná. I nadále je nezbytné, aby se dbalo na digitální hygienu. Díky tomu by občané dosáhli potřebné úrovně a začali naplno využívat moderní technologie a zároveň by došlo k minimalizaci nežádoucích kybernetických rizik. Vzdělávací systém musí začlenit problematiku kybernetické bezpečnosti do svých osnov. Je nutné posilovat informační gramotnost nejen u dětí, žáků a studentů, ale i u seniorů. Zejména poslední skupinu obyvatel je nezbytné edukovat v rozeznávání dezinformací a bezpečném používání digitálních technologií. ČR usiluje o zabezpečení digitální veřejné správy a zajištění kybernetické bezpečnosti v počáteční fázi výstavby. Potřebuje rozšiřovat expertní základnu, takže musí včas identifikovat talenty a motivovat lidi ke studiu a práci v oblasti kybernetické bezpečnost a poté si dokázat udržet své pracovníky v této oblasti. Cíle Národní strategie kybernetické bezpečnosti ČR jsou převedeny do konkrétních úkolů v rámci Akčního plánu a NÚKIB bude hodnotit a koordinovat plnění cílů (NÚKIB, 2020c).

5. Kybernetická cvičení na národní a mezinárodní úrovni

Aby NATO zvládlo čelit hrozbám v kyberprostoru, musí umět předcházet útokům na aliančí kyberprostor, bránit se před probíhajícími útoky a umět se z nich ponaučit. Vojenská kybernetická cvičení představují mnoho výzev a příležitostí pro získání nových znalostí, ale i dovedností a postupů nezbytných pro úspěšnou integraci do kybernetických operací (Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, & Thompson, 2019).

Kybernetická cvičení sehrávají významnou roli při zajišťování kybernetické bezpečnosti ČR. Umožňují věrně simulovat různé typy krizových situací a slouží jak technickému publiku, tak pracovníkům na nejvyšší úrovni s rozhodovacími pravomocemi. Při přípravě a následném provedení je zásadní úzká spolupráce s dalšími partnery v rámci tzv. whole-of-government přístupu. Cvičení nesou edukativní prvky a pomáhají také budovat důvěru a utužovat vzájemné vztahy. NÚKIB rozlišuje pět typů kybernetických cvičení: technická, table-top, procesní, komunikační a hybridní (NÚKIB. n.d.a).

Cvičení NÚKIB umožňují zjistit a upozornit na nedostatky nebo slabá místa v kyberprostoru. Použitím krizových scénářů umožňují lépe nastínit možné negativní dopady. Na základě zjištěných nedostatků přispívají ke zlepšení zabezpečení a jsou zdrojem nových znalostí, zkušeností a technických schopností. Získané výstupy a poznatky jsou dále využívány pro edukativní účely. Cvičení pomáhají zjišťovat aktuální stav kybernetické bezpečnosti a navrhovat prostředky k jeho zlepšení (NÚKIB. n.d.b).

5.1. Technické cvičení

„Tento typ je určen pro technické experty, tedy taktickou úroveň. Ti cvičí na určené infrastruktuře, kdy ji kupříkladu brání proti simulovaným útokům protivníka. Připravují se tak na reálnou krizovou situaci.“ (NÚKIB, n.d. c).

Pod názvem Cyber Czech se skrývá kybernetické bezpečnostní cvičení, které je jediným pravidelným cvičením v ČR. Cvičení využívá kombinaci technických i netechnických prostředků k vytvoření, co nejvíce realistické situace a probíhá v Kybernetickém polygonu (KYPO) Masarykovy univerzity ve spolupráci s NÚKIB. Na realizaci se podílí také Kyberbezpečností tým Masarykovy univerzity CSIRT-MU[17]. K cílům cvičení patří příprava bezpečnostních pracovníků na práci pod tlakem během probíhajícího útoku. V prostorech KYPO lze vytvářet jedinečné prostředí pro útoky se zaměřením na podnikové systémy, kritickou informační strukturu a další. *„KYPO umožňuje škálovat velikost útoků a zohlednit*

[17] První certifikovaný kyberbezpečnostní tým v ČR. (Masarykova univerzita, n.d.a)

rozsáhlé počítačové sítě včetně běžících aplikací a služeb.“ Každé cvičení je pozorně monitorováno, podrobně vyhodnocováno a analyzováno. Na konci cvičení přichází na řadu zpětná vazba, která obsahuje identifikaci všech chyb, vysvětlení nejlepšího vhodného postupu i doporučení. *„V rámci cvičení pracuje několik týmů obránců (obvykle šest čtyřčlenných týmů), vystavených identickému scénáři. Každý tým tedy řeší totožnou situaci se stejným cílem a řešení volí podle své strategie, znalostí a schopností. Za jednotlivé úkony získávají týmy obránců body. Hlavním účelem však není zvítězit, ale načerpat potřebné znalosti a schopnosti pro řešení podobných situací v praxi.“* Cvičení se krom IT expertů účastní i týmy např. odborníků na právo, PR apod. Důraz je kladen na realističnost celé situace (Masarykova univerzita. n.d.b).

Technické kybernetické bezpečnostní cvičení Crossed Swords organizuje NATO CCDCOE. Zaměřuje se zaměřuje na procvičení penetračních testerů, forenzních analytiků a utváření jejich situačního povědomí. K cílům cvičení patří rozvoj dovedností účastníků v oblastech prevence, detekce a reakce na kybernetické operace v jejich plném rozsahu. Mnoho účastníků tohoto kybernetického cvičení se následně stávají součástí Červeného týmu v rámci cvičení Locked Shields (CCDCOE, n.d.a).

5.2. Table-top cvičení

Jedná se o netechnický typ cvičení, který může mít různé podoby. K jednomu z nejčastějších typů patří cvičení, během kterého účastníci sedí u stolu a v rámci společné diskuze se snaží vyřešit předložený krizový scénář. Tento typ cvičení je ideální pro širokou škálu publika, od techniků po střední a vyšší management. K hlavním cílům table-top cvičení patří vzdělávání státních zaměstnanců na vedoucích pozicích, jejichž agenda obsahuje kybernetickou bezpečnost nebo jsou touto problematikou ovlivněni. Cvičení simulují různé krizové situace a scénáře. Z každého cvičení vyplývají cenné poznatky, které pomáhají při zvyšování kybernetické bezpečnosti v ČR. K cílům Table-top cvičení patří také vzdělávání studentů a osvěta odborné veřejnosti, zvyšování povědomí státních zaměstnanců o aktuálních českých i zahraničních přístupech a trendech v kybernetické bezpečnosti. ČR nezapomíná ani na své zahraniční partery a v rámci spolupráce s nimi sdílí získané know-how. (NÚKIB, n.d.c)

V roce 2019 se uskutečnilo první sektorové cvičení kybernetické bezpečnosti Electro Czech 2019. Cvičení probíhalo pod vedením NÚKIB a ve spolupráci s Českými energetickými závody (ČEZ). Historicky prvního sektorového cvičení kybernetické bezpečnosti se zúčastnilo více než 60 zástupců nejdůležitějších společností českého energetického sektoru. Cílem cvičení bylo zlepšit připravenost energetických společností na krizové situace, které mohou během kybernetických útoků nastat. *„Samotné cvičení probíhalo formou moderované diskuse. V jejím*

rámci účastníci navrhovali řešení různých předem připravených scénářů, které kombinovaly jak provozní závady, tak cílené kybernetické útoky či dezinformační kampaně. Otázky pro cvičící byly záměrně formulované tak, aby se cvičící zamýšleli nad technickými, právními, ale i mediálními aspekty zvládání krizových situací." Každý účastník si v praxi vyzkoušel rozhodovací postupy, vzájemnou spolupráci s účastníky z jiných společností a zároveň musel zvažovat právní možnosti. Průběh incidentů museli účastníci srozumitelně komunikovat s veřejností. Nechyběla ani simulovaná tisková konference za účasti reálného novináře a vysokých představitelů všech institucí působících v oblasti výroby, přenosu a distribuce elektřiny. *„Výsledkem cvičení byla expertní výměna názorů a přístupů jednotlivých organizací k řešení kybernetického bezpečnostního incidentu, identifikace bílých míst v rámci vzájemné koordinace a celkové posílení krizové připravenosti zúčastněných institucí."* (NÚKIB, n.d.d).

Od roku 2005 se v ČR koná Letní škola NATO pro postgraduální studenty politologie, mezinárodních vztahů a dalších příbuzných oborů z řad členských států a partnerských zemí NATO. Letní školu NATO organizuje Pražský institut bezpečnostních studií (PSSI), Týdenní kurz zahrnuje prezentace, přednášky, diskuse a simulace vedené českými i zahraničními bezpečnostními experty. Během jednoho týdne se odborníci snaží zájemcům přiblížit budoucí výzvy pro NATO a problémy globální bezpečnostní agendy. Účastníci se mohou setkat s představiteli NATO a předními bezpečnostními odborníky (Prague Security Studies Institute. n.d.).

Kybernetická cvičení probíhají také v Africe. V roce 2018 se český zúčastnil cvičení Africa Endeavour 2018 zaměřené na komunikaci, interoperabilitu a kybernetickou bezpečnost. Čeští zástupci se zúčastnili panelu věnovaného ochraně kritické infrastruktury a s kolegy si vyměnili rady a poznatky. Český tým provedl netechnické table-top cvičení, což bylo přínosné pro všechny zúčastněné. Účastníci byli rozdělení do malých skupin a zabývali se DDoS útokem, narušením sítě ministerstva nebo kybernetickým útokem na rozvodnou síť. Po skončení cvičení následovalo hodnocení a zpětná vazba (Národní centrum kybernetické bezpečnosti. n.d.a).

5.3. Procesní cvičení

V rámci procesního cvičení se procvičují vybrané procesy v oblasti kybernetické bezpečnosti, jako jsou reakce organizací na kybernetické útoky. Aby simulované cvičení, co nejvěrohodněji, zprostředkovalo cvičícím práci s kybernetickou hrozbu, probíhají tato cvičení na reálném pracovišti. Pozornost je upřena na rozhodovací procesy, interní postupy a komunikaci. NATO, ve spolupráci s NATO CCDCOE, každoročně pořádá pětidenní cvičení

Cyber Coalition[18], což je jedno z největších kolektivních kybernetických cvičení na světě. Procesní cvičení je řízeno z estonského města Tartu a patří k největším a nejvýznamnějším cvičením tohoto druhu. Pod vedením Vojenského výboru NATO je cvičení plánováno a řízeno Velitelstvím spojeneckých sil pro transformaci. Do cvičení se zapojují stovky odborníků z členských a partnerských zemí, včetně institucí EU a odborníků ze soukromého i akademického sektoru. Hlavním cílem cvičení je procvičení spolupráce a koordinace během probíhajících simulovaných kybernetických bezpečnostních incidentů napříč státy a jednotlivými sektory. Samozřejmostí je také nalezení správného řešení. ČR na cvičení zastupuje NÚKIB a Ministerstvo obrany (NÚKIB, n.d.c). *„Kybernetická koalice, která se koná každoročně od roku 2008, sdružuje kybernetickou koalici orgánů NATO, spojenců a partnerů NATO, aby posílila schopnost Aliance odstrašovat, bránit se a čelit hrozbám v kybernetickém prostoru.“* (NATO, n.d.a).

„Cyber Coalition je založeno na komplexním a realistickém scénáři, kdy se silný aktér snaží ohrozit misi Aliance a dosáhnout svých cílů prováděním pokročilých a sofistikovaných kybernetických operací. Jejich řešení si vyžaduje koordinaci a spolupráci zúčastněných expertů NATO, jeho členských států a partnerů.“ Připravený scénář pomáhá připravit účastníky na skutečné kybernetické výzvy, do kterých jsou zahrnuty útoky na kritickou infrastrukturu i narušení činnosti NATO a spojenců během operací. V rámci cvičení je používán tzv. cyber range, což je virtualizované prostředí, které simuluje síťovou infrastrukturu a dodává tak cvičení na realističnosti (NÚKIB, 2022b).

5.4. Komunikační cvičení

Komunikační cvičení si klade za cíl kontrolu komunikačních kanálů, aby byly připraveny pro případ krize. Efektivní, rychlá a bezpečná komunikace mezi státním a soukromým sektorem je zásadní během probíhající krize. Příkladem komunikačního typu cvičení je cvičení Comm Czech.

V roce 2018 se cvičení zaměřilo na subjekty kritické informační infrastruktury a významných informačních systémů. *„Cílem Comm Czechu bylo prověřit dostupnost nastavených komunikačních kanálů a zjistit, zda jsou nahlášené kontaktní údaje v souladu s § 16 zákona o kybernetické bezpečnosti.“* Cvičení bylo rozděleno do dvou fází. V první fázi se zkoušela elektronická komunikace a ověřovala se aktuálnost uvedených e-mailových adres.

[18] Cyber Coalition v českém překladu Kybernetická koalice

Ve druhé fázi se ověřovala správnost a dostupnost nahlášených kontaktních údajů prostřednictvím telefonického hovoru (NÚKIB, 2018a).

V květnu 2013 byla založena Cyber Security Platform (CECSP) z iniciativy Rakouska a ČR. Skládá se ze zástupců národních bezpečnostních orgánů a národních center kybernetické bezpečnosti ze Slovenska, České republiky, Polska, Maďarska a Rakouska spolu se zástupci z národních, vládních, a vojenských týmů. (Národný bezpečnostný úrad Slovenské republiky. n.d.). Cílem platformy je intenzivní spolupráce sousedních zemích a sdílení osvědčených postupů, informací, zkušeností, know-how o kybernetických hrozbách a potenciálních nebo úspěšně či neúspěšně provedených kybernetických útocích. Platforma dále přispěje k budování kapacit a kompetencí, a to prostřednictvím společných školení, vzdělávání, cvičení a koordinace výzkumu a vývoje. V neposlední řadě zúčastněné státy usilují o harmonizované pozice v mezinárodním prostředí (ENISA. n.d.).

5.5. Hybridní cvičení

Hybridní cvičení kombinuje roviny technické, rozhodovací, právní i mediální. Cvičení dokáže nejvěrněji simulovat reálnou krizovou situaci a účastní se ho cvičící od taktické až po strategickou úroveň. Během 15. ročníku, v roce 2022, se do hlavního města Estonska – Tallinnu sjelo více než tisíc expertů a zástupců soukromého a veřejného sektoru z 26 členských států NATO a sedmi partnerských zemí. Jednoho z největších a nejvýznamnějších světových cvičení na kybernetickou bezpečnost se účastnilo také 14 českých odborníků z Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Čeští účastníci pracovali a trénovali spolupráci a kooperaci během řešení kybernetických incidentů napříč jednotlivými sektory a státy (NÚKIB, 2022b).

Locked Shields je každoroční cvičení pořádané od roku 2010. Cvičení poskytuje odborníkům na kybernetickou bezpečnost zlepšit své znalosti a dovednosti při obraně národních IT systémů a kritické infrastruktury před útoky v reálném čase. Během cvičení se používají špičkové technologie, realistické scénáře a simulace masivních kybernetických útoků, včetně strategického rozhodování, právních a komunikačních aspektů. Stojí proti sobě tzv. Červený tým versus Modrý tým. Červený tým má roli útočníka a Modrý tým tvoří členské státy a partneři CCDCOE (CCDCOE n.d.c).

„Česká republika bývá zastoupena jak v Modrém soutěžním týmu, v Bílém organizačním týmu, v Zeleném týmu zodpovědném za infrastrukturu, tak v Červeném týmu útočníků. Národní tým je složen ze zaměstnanců NÚKIB a zástupců dalších subjektů bezpečnostní komunity státní, soukromé i akademické sféry.“ NÚKIB pomáhá s přípravou cvičení v rámci plánovacích týmů,

což je pro všechny zaměstnance jedinečnou zkušenosti, kterou mohou zúročit při přípravě cvičení na národní úrovni (NÚKIB, n.d.c).

Cvičení testuje komplexní otázky týkající se právních, technických, analytických a komunikačních otázek. Aby týmy uspěly, musí správně vyhodnotit složité otázky z oblasti mezinárodního práva, včas a správně identifikovat dezinformace a provést analýzy mediálního prostředí. Součástí týmu je i strategický tým, jenž vykonává rozhodnutí na strategické úrovni, a proto je velice důležitá kvalitní koordinace v rámci mezi všemi členy týmu. Český národní tým v posledních letech dosahuje skvělých výsledků a umisťuje se na předních příčkách úspěšnosti (Euroskop, NÚKIB, Pixabay.com & Pospíšil, 2022). Na tvorbě politiky EU v oblasti kybernetické bezpečnosti se podílí také Evropská agentura pro bezpečnost sítí a informací (ENISA). Vytváří systémy certifikace kybernetické bezpečnosti a zajišťuje větší důvěru v služby a procesy a digitální produkty. Spolupracuje s orgány a zeměmi EU a pomáhá jim s přípravou na budoucí kybernetické výzvy.“ (Evropská unie. n.d.). Již 15 let organizuje místní, mezinárodní a celoevropská kybernetická cvičení. Vyvíjí také platformy pro kybernetická cvičení, aby zúčastněné strany mohly pořádat svá vlastní cvičení. ENISA pořádá cvičení Cyber Europe, které je největším cvičením ENISA a sdružuje krizové specialisty ze soukromého a veřejného sektoru Koncept se zaměřuje na analýzu a snaží se odrazit kybernetický útok na konkrétní zranitelný sektor, který by mohl být hrozbou pro národní bezpečnost. ENISA provádí co nejvíce realistické simulace k testování kritické bezpečnostní infrastruktury EU a snaží se koordinovat reakce na kybernetický útok přes hranice v rámci Unie (European Union Agency for Cybersecurity. n.d.b).

V roce 2022 organizátoři cvičení předložili scénář, který se zaměřil na zdravotnictví a zahrnoval nemocnice, kliniky, ministerstvo zdravotnictví, zdravotní pojišťovny apod. Účastníci cvičení tak měli jedinečnou možnost vyzkoušet si řešení incidentu, který přerostl ve velkou krizi (European Union Agency for Cybersecurity. n.d.a).

5.6. Trident Juncture

Od 25. října do 7. listopadu 2018 probíhalo v Norsku a okolní oblasti severního Atlantiku a Baltského moře největší bezpečnostní cvičením NATO od roku 2002 - Trident Juncture. Během tohoto cvičení spojenci a partnerské země testovali schopnost spolupracovat při obraně území a obyvatelstva členských zemí a zastrašování potenciálních protivníků ohrožující kyberbezpečnost. Cvičení se zúčastnilo přibližně 50 000 účastníků (NATO, 2018).

Cvičení Trident Juncture se zúčastnili také čeští vojáci převážně z 25. protiletadlového raketového pluku ze Strakonic. Jejich úkolem bylo zabezpečit pozemní protivzdušnou obranu

mechanizovaným i tankovým praporům a taktickému místu velení obrněné brigády. Účastníci měli možnost porovnat své operační postupy s postupy, které používají alianční partneři a vyměnit si mezi sebou zkušenosti na všech stupních velení a řízení operace. Cvičení probíhalo na civilním území, což v ČR nebývá zvykem a vojáci si musel zvyknout na nevojenské prostory (Samcová, 2018). Cvičení NATO trénuje vojáky, vyhodnocuje operace a jejich reakce na krizové situace zahrnující bojové schopnosti v raných fázích operací. CDCOE poskytla kybernetické experty v oblasti vývoje a skriptování, plánování reakce na krizové situace, školení, hodnocení apod. (NATO Cooperative Cyber Defence Centre of Excellence, n.d.b).

6. Kybernetické útoky na kritickou infrastrukturu ČR v letech 2013-2022

Kybernetické útoky s sebou nesou mnoho výhod. První výhodou je, že kybernetický útok může být selektivní a rozsah následků může být kontrolovaný. Kybernetický útok by se mohl zaměřit např. pouze na ekonomiku země, aniž by zničil kritickou infrastrukturu. Další možností je, že by útok cílil na kritickou infrastrukturu státu spolu s jeho ekonomikou. Útok zacílený na ekonomickou oblast může stát oslabit a způsobit paniku mezi občany. Druhou výhodou je, že kybernetický útok nevyžaduje nasazení několika agentů, které by zvýšilo riziko odhalení a dopadení bezpečnostními složkami. Útok může být smrtelný, ale zároveň představuje méně rizik spojených s odhalením a selháním. Třetí výhodou jsou také nižší finanční náklady, jelikož odpadají náklady na konvenční zbraně a operační riziko. Počítačové botnety si útočníci mohou koupit za pár tisíc dolarů a způsobit škody stonásobně větší. Čtvrtou výhodou je, že zločinec si může zvolit čas, místo a nástroj zločinu. Útočník je často odborníkem na způsob provedení trestného činu. Obránce napadeného kyberprostoru má často znalosti z řady oblastí, ale v omezeném množství. Pátý bod představuje neomezené hranice kyberzločinu. Opatření přijatá v rámci bezpečnosti jednoho státu nemusí stačit a útok může překročit mezistátní a mezinárodní hranice. Většina donucovacích orgánů má geografické limity, které zahrnují jejich jurisdikci. Překročení těchto limitů vyžaduje koordinaci s dalšími orgány, které se nemusí názorově shodovat nebo nemusí cítit naléhavost spolupracovat (Syed, Khaver, & Yasin, 2019).

Začátkem března 2013 byly zaznamenány tři vlny DDoS útoky na některá média, portál Seznam.cz, mobilní operátory a banky. Jednalo se o významný sofistikovaný kybernetický útok, který v první vlně paralyzoval české zpravodajské servery (denik.cz, idnes.cz, ihned a další). Druhá vlna útoku zasáhla portál seznam.cz a třetí vlna cílila na bankovní instituce, konkrétně na Českou spořitelnu a zpětně byly nahlášeny incidenty o útocích na další banky (NÚKIB, 2014). K útoku se nikdo nepřihlásil (Hromádka, Kko, & Malínská, 2016). Škody byly vyčísleny na miliony korun (Česká televize, 2013).

V srpnu ústřední orgán státní správy nahlásil hackerský útok zaměřený na poštovní e- mailový server státní správy. V tomto roce se ČR zapojila do cvičení NATO. Uskutečnilo se cvičení Crisis Management Exercise, které se konalo i v roce 2012 a zahrnovalo kybernetické scénáře, ve kterých se testovala připravenost vojenských i civilních složek na reálné hrozby. Poprvé se ČR zapojila do cvičení Cyber Coalition, které mělo za cíl otestovat připravenost států NATO na probíhající hrozby v oblasti kybernetické bezpečnosti. Vláda schválila zapojení ČR do NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu (NÚKIB, 2014).

Rok 2014 se podobal roku 2013. Nejčastějším typem útoků byly DDoS útoky a phishing. Závažnější útok se stal v březnu, kdy došlo ke krádeži přihlašovacích údajů k webovým stránkám, sociálním sítím, e-mailovým účtům a jiným službám. Útočníkům se podařilo odcizit více než 700 000 uživatelských pověření. Ve statistikách tohoto roku se objevily také špionážní malwary a rozesílání podvodných emailů. *„Ředitel NBÚ podepsal dne 14. března 2012 Memorandum o porozumění (Memorandum of Understanding) s NATO ve věci kybernetické obrany. S ohledem na měnící se bezpečnostní paradigma započala v roce 2014 práce na sjednoceném znění tohoto Memoranda, které upravuje podmínky spolupráce v rámci alianční kybernetické obrany.“* Čeští zástupci se zúčastnili šesti kybernetických cvičení – CECSP 2014 Exercise, Cyber Czech14, Cyber Europe, Cyber Coalition., EU-Multi Layer a Locked Shields (NÚKIB, 2015).

V roce 2015 nejčastějšími cíli byli zákazníci e-shopů, bank, zaměstnanci státní správy a další skupiny. I v tomto případě byly opět objeveny šifrovací malwary. Třetí čtvrtletí roku se neslo ve znamení nárůstu infikace počítačů institucí státní správy ransomware a byla zaznamenána phishingová kampaň, která cílila na státní instituce. Došlo k upevňování a prohlubování vztahů s NATO. Národní bezpečnostní úřad se podílel na přípravě nového formátu memoranda o porozumění s NATO o spolupráci v oblasti kybernetické obrany. Dne 12. října 2015 byla ČR první členskou zemí NATO, která toto memorandum podepsal. *„Česká republika se aktivně podílela rovněž na činnosti NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) v estonském Tallinnu, jehož posláním je výzkumná a vědecká činnost v oblasti kybernetické bezpečnosti a obrany, a zlepšování spolupráce a sdílení informací mezi členskými státy a NATO.“* V roce 2015 se NBÚ zúčastnil čtyř mezinárodních cvičení – Crisis Management Exercise, Locked Shields, Cyber Coalition a CECSP 2015 (NÚKIB, 2016).

V roce 2016 bylo zaznamenáno 298 relevantních kybernetických bezpečnostních incidentů. V prvním čtvrtletí roku byly zaznamenané četné malwarové útoky, útočníci rozesílali podvodné zprávy se škodlivými přílohami a cílili na zákazníky bank, zaměstnance státní správy a další skupiny. Ve druhém čtvrtletí roku převažovaly DDoS a phishingové útoky, které cílily na státní instituce, webové stránky politických subjektů a veřejnoprávní média. Na konci roku se řešily různé typy incidentů, výskyty ransomware, zranitelnosti a ojedinělé DDoS útoky na instituce státní správy. Významnou událostí bylo uznání kybernetického prostoru jako další operační domény nejvyššími představiteli členských států během summitu NATO ve Varšavě. Na summitu byl přijat dokument Cyber Defence Pledge, který zavazuje státy budovat a posilovat bezpečnost národních sítí a informační infrastruktury a tím navýšit odolnost států i celé Aliance proti kybernetickým útokům. ČR se opět účastnila mezinárodních cvičení –

Locked Shields, Cyber Coalition, Cyber Europe a NATO CMX 2016. NBÚ uspořádal dvě cvičení pro zahraniční partnery (NÚKIB, 2017).

248 relevantních hlášení o kybernetických bezpečnostních incidentech bylo zaznamenáno v roce 2017. V tomto roce pokračoval trend phishingových a DDoS útoků a vyděračské e-maily. Konaly se volby do Poslanecké sněmovny a očekávalo se, že by mohlo dojít ke kybernetickému útoku. Byl zaznamenán DDoS útok na servery volbyhned.cz, volby.cz a webovou prezentaci ČSÚ, které poskytují přehled o průběžných výsledcích sčítání, nedošlo k narušení sčítání ani výsledků voleb (NÚKIB, 2018b). Nejméně 150 zemí zasáhl masivní kybernetický útok ransomware WannaCry. Útok byl neobvyklý svým rozsahem a rychlostí, s jakou se po světě šířil. Kromě nákazy prostřednictvím přílohy e-mailů, ransomware využil chybu ve starších operačních systémech Windows k šíření po lokální síti. Útok zasáhl např. počítače zdravotnických zařízení ve Velké Británii a došlo tak k omezení poskytované lékařské péče. Útok se zasáhl i české počítače, avšak nedošlo k zasažení institucí (ČTK, iDNES.cz., Kasík & Lázňovský, 2017). Útoky zasáhly také Čínu, kde ransomware napadl počítače na některých středních školách a univerzitách. V Rusku virus ochromil ministerstvo vnitra, dokonce i ruskou banku Sberbank. Útok zasáhl řadu velkých španělských firem, jako je telekomunikační gigant Telefonica, energetická firma Iberdrola a poskytovatel veřejných služeb Gas Natural. Zasaženy byly ale i další velké firmy a instituce, a to včetně dodavatelské služby FedEx, francouzské automobilky Renault či počítače německých železnic (BBC News, 2017).

V roce 2018 bylo nahlášeno 164 relevantních nahlášených kybernetických bezpečnostních incidentů. Největší procento útoků tvořily DDoS útoky, phishing a škodlivý obsah (např. trojský kůň, virus, červ apod.). Taktéž v tomto roce se ČR zúčastnila tří mezinárodních cvičení (NÚKIB, 2019).

V průběhu roku 2019 bylo nahlášeno 217 relevantních kybernetických bezpečnostních incidentů. Oproti roku 2018 došlo k nárustu nahlášených incidentů. Trendem tohoto roku byly sofistikovanější škodlivé e-maily a DDoS útoky. Nejvážnějším incidentem tohoto roku bylo infikování systémů Nemocnice Rudolfa a Stefanie Benešov a těžební společnosti OKD ransomwarem Ryuk (NÚKIB, 2020b). Během kybernetického útoku na těžební firmu OKD hackeři ochromili počítačovou síť společnosti. Útok způsobil nefunkčnost celé sítě těžařské firmy a všech jejích serverů. Mimo provoz se ocitla kompletní síťová infrastruktura a z bezpečnostních důvodů vedení společnosti OKD okamžitě ukončilo těžbu ve všech svých dolech. (Česká televize 2019). NÚKIB vyslal na pomoc tým odborníků, kteří pomáhali s obnovou informační sítě, forenzní a síťovou analýzou a s nastavením základních

bezpečnostních. Odhadovaná škoda byla vyčíslena na více než 5 milionů korun (ČTK, 2020). Dalším incidentem bylo infikování státní instituce malwarem Emotet. ČR se i v tomto roce účastnila cvičení NATO. Český tým si ze cvičení Locked Shields odvezl domů druhé místo (NÚKIB, 2020b).

V roce 2020 bylo nahlášeno 468 incidentů, což je skokový nárůst oproti předchozímu roku. Vzrostla závažnost nahlášených incidentů. Proběl ransomwarový útok na Fakultní nemocnici Brno, ale i na Psychiatrickou nemocnici Kosmonosy. Útok vyřadil několik IT systémů nemocnice. Kvůli odpojení počítačů nemohly být prováděny operace, nefungovaly počítače s uloženými daty pacientů a pacienti museli být převezeni na operace do okolních nemocnicích. (Právo, 2020). Škoda byla předběžně vyčíslená na 150 milionů korun (Horák, 2021). Nejčastějšími typy útoků v tomto roce byly phishing, spam a scanning. NÚKIB v roce 2020 pořádal či koordinoval osm národních a mezinárodních cvičení. I přes probíhající pandemii Covid-19 se ČR alespoň virtuálně zúčastnila cvičení NATO – Cyber Coalition. NÚKIB uspořádal komunikační cvičení Comm Czech 2020 (NÚKIB, 2021).

V roce 2021 NÚKIB evidoval 157 kybernetických bezpečnostních incidentů oproti roku 2020, kdy jich bylo zaznamenáno 99, což značí nárust o 58 incidentů. V roce 2021 nejčastějšími typy útoků byly podvodné e-maily, skenování vnější sítě a phishing. V tomto roce kybernetickou bezpečnost v ČR i v zahraničí narušovala zranitelnost ProxyLogon, ProxyShell a Log4Shell. Tak jako v minulých letech čelily subjekty kritické informační infrastruktury až tisícům pokusů o kybernetický útok, avšak celkový počet incidentů v této kategorii se meziročně snížil přibližně o čtvrtinu. Narostl však podíl incidentů, které omezily dostupnost služeb. Veřejný sektor patřil k sektorům, které byly nejvíce zasaženy. Téměř polovina (40 %) všech kybernetických bezpečnostních incidentů, které NÚKIB zaznamenal, se odehrála ve veřejném sektoru a počet incidentů v tomto sektoru stále narůstá. Nejčastějšími typy útoků ve veřejném sektoru byly phishing, podvodné emaily a skenování vnější sítě. *„Český finanční sektor bývá označován za jedno z nejlépe zabezpečených odvětví, čemuž nasvědčuje také absence vážnějších incidentů v roce 2021.“* Sektor průmyslu a energetiky čelil zejména masivním ransomwarovým útokům nejen v Česku, ale i v mezinárodním prostředí. Kvůli ransomwarovému útoku[19] musela být zastavena výroba jednoho z dodavatelů pro energetický sektor ČR. *„Počet incidentů ve zdravotnictví registrovaných NÚKIB se meziročně zvýšil o 34 %, přičemž až polovina incidentů byla hodnocena jako významná či velmi významná.“* Vzdělávací sektor zaznamenal šestinásobný nárůst incidentů evidovaných NÚKIB (NÚKIB,

[19] Ransomwarový útok je považován za jednu z nejzávažnějších hrozeb pro průmyslový a energetický sektor, jelikož zajištění kontinuity produkce a poskytování služeb je jejich prioritním cílem. (NÚKIB, 2022a)

2022a). Nejvýznamnějším kybernetickým útokem tohoto roku se stal útok na jednu z největších veřejných institucí v Česku, a to na Národní knihovnu. Po zjištění útoku knihovna odpojila klíčové systémy a odborníci pracovali na znovu zprovoznění. Útokem se zabýval také NÚKIB, kterému Knihovna nahlásila incident (ČTK, (2021). V tomto roce se konalo několik kybernetických cvičení. Uskutečnilo se největší cvičení kybernetické bezpečnosti na světě s názvem Locked Shields 2021. Dalšími mezinárodními cvičeními, které se uskutečnily, byly Cyber Coalition a CRISIS-X. CRISIS-X bylo prvním společným cvičením NÚKIB a Israel National Cyber Directorate, v jehož prostřednictvím si týmy prověřili schopnost zvládání incidentů na národní úrovni a také vzájemnou komunikaci (NÚKIB, 2022a).

Zvýšené riziko kybernetických útoků v ČR způsobuje od února 2022 válka na Ukrajině[20]. Od října 2022 byl zaznamenán nárůst kybernetických útoků v ČR a ve státech NATO. Přibližně po třech měsících od začátku invaze se začal zvyšovat počet útoků ve státech NATO. Nejčastějšími cíli ruských hackerů jsou česká ministerstva, nemocnice a vzdělávací instituce (Andrle, 2023).

Na Ředitelství silnic a dálnic (ŘSD) v roce 2022 zaútočili hackeři, kterým se podařilo zašifrovat data a znepřístupnit webové stránky ŘSD a internetovou stránku Dopravniinfo.cz. Hackeři požadovali výkupné za odšifrování dat ŘSD, které se ale nakonec nezaplatilo. Útok vyřadil z provozu zhruba 1000 serverů a všechny aplikace. Náklady na obnovu informačních systémů a zvýšení zabezpečení se pohybují kolem 30 milionů Kč. Tento kybernetický útok splňuje druhé kritérium, jelikož škody způsobené sofistikovaným ransomwarem se vyšplhaly do řádu několika milionů korun. Nikdo nebyl ohrožen na životě a nebyla vyžádána pomoc NATO. (ČTK, 2022). NÚKIB vydal varování před zvýšeným rizikem kybernetických útoků typu DDoS (Distributed Denial of Service) Během útoku DDoS tisíce počítačů začnou přistupovat v jeden okamžik na vybraný server, který zpravidla nezvládne tak vysoké množství požadavků zpracovat a spadne. Pro běžné uživatele se pak napadená webová stránka tváří jako nedostupná. DDoS útoky většinou mívají pouze krátkodobý dopad (Husák, 2022).

[20] Ruská invaze na Ukrajinu začala 24. února 2022 (CNN, 2023).

7. Role NATO v boji proti kybernetickým útokům

Z dat prezentovaných ve zprávách o stavu kybernetické bezpečnosti v letech 2013–2021 vyplývá, že ČR se pravidelně účastní cvičení NATO, která jsou zaměřena na kybernetiku. NATO pomáhá zlepšit národní kybernetickou obranu svých spojenců prostřednictvím sdílení informací, osvědčených postupů a zkušeností. Pravidelně organizuje cvičení zaměřená na kybernetickou obranu za účelem rozvoje odborných znalostí v této oblasti (NATO, n.d.b).

Ve zprávách o stavu kybernetické bezpečnosti se také uvádí, že v ČR dosud nedošlo k natolik závažnému kybernetickému útoků, do kterého by se NATO zapojilo. Primární odpovědnost za reakci na hybridní hrozby nebo útoky spočívá na zasažené zemi, avšak NATO je připraveno bránit své spojence, včetně ČR, před jakoukoli hrozbou. Kybernetický útok proti jednomu nebo více spojencům by mohl vést k rozhodnutí aktivovat Článek pět Severoatlantické smlouvy. Článek pět představuje dohodu smluvních stran, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem členům NATO. Smluvní strany odsouhlasily, že dojde-li k ozbrojenému útoku, každá z nich uplatní právo

na individuální nebo kolektivní obranu, uznané článkem 51 Charty OSN, pomůže napadené straně nebo stranám a podnikne takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a udržet bezpečnost severoatlantické oblasti. Každý útok a všechna opatření budou neprodleně oznámena Radě bezpečnosti. Jakmile Rada bezpečnosti přijme nezbytná usnesení, která jsou nezbytná pro obnovení a zachování mezinárodního míru a bezpečnosti, tak tehdy přijatá opatření jsou ukončena. NATO je připravené pomoci jakémukoli spojenci v boji proti hybridním hrozbám v rámci kolektivní obrany. NATO disponuje vlastní strategii pro boj v hybridní válce a jeho úkolem je zajistit, aby celá Aliance i spojenci byli připraveni čelit kybernetickým útokům. NATO neustále shromažďuje, sdílí a vyhodnocuje informace, aby bylo připravené včas detekovat hybridní hrozby (NATO, n.d.c),

Na zasedání NATO v červnu 2016 byl kyberprostor uznán jako operační doména a toto rozhodnutí bylo znovu potvrzeno na summitu NATO ve Varšavě v červenci 2016. Po uznání kyberprostoru jako nové operační domény NATO, Aliance schválila plán pro kyberprostor, zřídila nové kybernetické operační centrum (CyOC), souhlasila s vojenskou strategií pro operace v kyberprostoru a přijala mnoho dalších opatření. (Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, & Thompson, 2019). Na varšavském summitu se spojenci zavázali k posílení a zlepšení kybernetické obrany národních sítí a infrastruktur. Na summitu NATO v Bruselu v roce 2021 byla schválena nová komplexní politika kybernetické obrany, která

podporuje tři základní úkoly NATO, mezi které patří krizové řízení, kolektivní obrana, kooperativní bezpečnost, odstrašování a obranná pozice. Reakce na kybernetický útok vychází ze souboru nástrojů NATO, které zahrnují politické, diplomatické a vojenské nástroje (NATO, 2023b).

Ve druhé kapitole byly představeny orgány NATO specializující se na obranu kyberprostoru a na boj proti kyberútokům. Tyto orgány poskytují podporu v kybernetické obraně členským zemím a jsou připravené pomoct ČR v případě kybernetického útoku na kritickou infrastrukturu.

Aby NATO rozvíjela své schopností v oblasti kybernetické obrany, NATO definovala cíle a schopnosti, kterých by členové a partneři měli dosáhnout, v dokumentu NATO Defence Planning Process[21]. NATO pomáhá zlepšit národní kybernetickou obranu svých spojenců prostřednictvím sdílení informací, osvědčených postupů a zkušeností. Pravidelně organizuje cvičení zaměřené na kybernetickou obranu za účelem rozvoje odborných znalostí v této oblasti. NCI Academy[22] nabízí školení a vzdělávání v oblasti kybernetické obrany. Škola NATO v Oberammergau v Německu poskytuje vzdělání a výcvik v kybernetické obraně a kybernetických operacích. NATO Defense College v italském Římě podporuje strategické myšlení o politicko-vojenských záležitostech a otázkách kybernetické obrany (NATO, n.d.b).

NATO spolupracuje také s Evropskou unií (EU), Organizací spojených národů (OSN) a Organizací pro bezpečnost a spolupráci v Evropě (OBSE). Kybernetická obrana je jednou z oblastí, ve které je posílená spolupráce mezi NATO a EU. NATO a EU mezi sebou sdílejí informace a osvědčené postupy. Prohlubují vzájemnou spolupráci v oblasti výzkumu, edukace a cvičení v boji proti kybernetickým hrozbám (NATO, n.d.b).

Prostřednictvím NATO Industry Cyber Partnership (NICP) se NATO a jeho spojenci snaží posílit vztahy s průmyslem a akademickou sférou, aby mohli využít inovace a držet krok s technologickým pokrokem. Toto partnerství zahrnuje subjekty NATO, národní týmy pro reakci na počítačové hrozby (CERT) a zástupce z průmyslu. Průmysl vytváří prostoru pro zlepšení schopnosti v kybernetické obraně. Sdílení informací, vzdělávání a cvičení je jen několik příkladů z oblastí, ve kterých NATO a průmysl spolupracují. (NATO, n.d.b). V návaznosti na spolupráci s průmyslem Rada NATO pro kontrolu dat a umělé inteligence[23] začala připravovat certifikační standard umělé inteligence, který pomůže průmyslovým odvětvím a institucím v rámci NATO zajistit, aby nová umělá inteligence a datové projekty

[21] Proces obraného plánování NATO
[22] NATO Communications and Information Academy
[23] Data and Artificial Intelligence Review Board

byly v souladu s mezinárodním právem, normami a hodnotami NATO. Norma, která se vztahuje na využívání dat, bude zahrnovat kontroly kvality. Rada je složena z nominovaných zástupců členských zemí, Finska a Švédska a také expertů NATO. Mezi zástupci se objevují právníci, odborníci na etiku, inženýři a vojenský personál. NATO v současné době využívá umělou inteligenci v oblastech, jako je změna klimatu, kybernetická obrana a analýza snímků (NATO, 2023a).

8. Strategie kybernetické obrany ČR

NCKO vydala Strategii kybernetické obrany České republiky pro období 2018–2022, která stanovuje podmínky pro zajišťování obrany státu v kybernetickém prostoru. Dokument definuje základní cíle, které popisují plánovaný vývoj kybernetické obrany v jednotlivých oblastech (Riethofová, n.d.).

Budování obranných schopností v oblasti kybernetiky je pro ČR důležité i s ohledem na členství v NATO, neboť kyberprostor byl uznán jako další operační doména, což znamená, že kybernetický útok může aktivovat Článek pět Severoatlantické smlouvy. Proto v souladu s požadavkem v Článku tři Severoatlantické smlouvy by smluvní strany měly udržovat a rozvíjet schopnosti odolat kybernetickým útokům. ČR uvedené požadavky reflektuje a postupně přijímá potřebná opatření, aby byla schopna odolat kyberútokům. K aktivaci kybernetické obrany může dojít pouze v případě těch nejintenzivnějších útoků. Kybernetická obrana bude prováděna jak v případě vyhlášení mimořádných stavů, především formou součinnosti s ostatními složkami zajišťujícími obranu ČR, tak i nepřetržitě mimo tyto stavy. *„Strategie kybernetické obrany za svůj globální cíl považuje dosažení takového stavu, kdy NCKO bude zajišťovat kybernetickou obranu ČR, bude schopné provádět vojenské operace v kybernetickém prostoru a zároveň plnit aktivní úlohu v mezinárodním prostředí“.* Aby došlo k naplnění globálního cíle, musí být prvně dosaženo strategických cílů, které jsou popsány ve Strategii kybernetické obrany ČR. Prvním strategickým cílem je nastavení právního rámce souvisejícího se zajištěním kybernetické obrany ČR. Po splnění tohoto prvního cíle budou vymezeny základní právní aspekty kybernetické obrany. Druhým cílem je vybudování a rozvoj infrastruktury NCKO. K prioritám patří obsazení NCKO kvalitním personálem, vyškolení a následné udržení kvalifikovaného a zkušeného personálu. V neposlední řadě také pořízení a vývoj špičkových technologií. Třetím úkolem je vybudování schopností obrany v kyberprostoru. ČR musí být schopna předvídat potencionální útoky, provádět operace v kyberprostoru v rámci kybernetické obrany a vojenských operací. Nabyté schopnosti budou poté ukotveny v doktrinálním rámci. Důležitou oblastí kybernetické obrany bude vytvoření tzv. „cyber deterrence“ strategie. Splněním třetího strategického cíle bude NCKO schopné aktivně působit v kybernetickém prostoru. Čtvrtým cílem je nastavení spolupráce a provádění vzdělávání a cvičení. NCKO musí vybudovat silná spojenectví v mezinárodním prostředí, zejména v rámci NATO, EU a s okolními zeměmi. NCKO musí rozvíjet spolupráci se soukromým sektorem, především v oblasti vědy a výzkumu. Významnou součástí spolupráce bude organizování či účast na cvičeních a vzdělávacích aktivitách. Po naplnění čtvrtého cíle dojde ke zkvalitnění zajišťování kybernetické obrany ČR. Pátým cílem je podílení se

na zajištění kybernetické bezpečnosti v rezortu MO. Úkolem všech složek v rámci rezortu Ministerstva obrany musí být zvýšení úrovně kybernetické bezpečnosti. Úkolem NCKO bude zajištění kybernetické bezpečnosti vlastních prostředků a sítí. Speciální schopnosti NCKO budou využity k posílení obranyschopnosti příslušníků rezortu Ministerstva obrany. Splněním tohoto cíle bude zajištěna spolehlivost a důvěryhodnost informačních systémů NCKO, včetně informačních systémů rezortu ministerstva. Plnění stanovených cílů strategie bude průběžně kontrolováno a vyhodnocováno. Strategie slouží k vybudování účinného systému kybernetické obrany v ČR v souladu s požadavky NATO. Získané zkušenosti se stanou podkladem pro plánování dalšího rozvoje (Národní centrum kybernetických operací, 2018).

Závěr

V letech 2013–2022 na kritickou infrastrukturu ČR cílilo několik významných kybernetických útoků, avšak žádný z nich nebyl natolik závažný, aby došlo k aktivaci Článku 5 Severoatlantické smlouvy a přímého zapojení NATO. Článek pět poskytuje odpověď na výzkumnou otázku *„Jakou pomoc poskytuje NATO členským zemím na základě oficiálních dokumentů v boji proti kybernetickým útokům?“* Článek pět představuje dohodu smluvních stran, že ozbrojený útok proti jednomu nebo více členům bude považován za útok proti všem členům NATO. Smluvní strany odsouhlasily, že dojde-li k ozbrojenému útoku, každá z nich uplatní právo na individuální nebo kolektivní obranu a pomůže napadené zemi nebo zemím a podnikne takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a udržet bezpečnost severoatlantické oblasti. NATO je připravená pomoci jakémukoli spojenci v boji proti hybridním hrozbám v rámci kolektivní obrany.

Krom Článku pět NATO nabízí také možnost vzdělání v oblasti kybernetické obrany na škole NATO v Německu a na škole NATO Defense College v Itálii. V oblasti kybernetické obrany NATO posílila svou spolupráci s Evropskou unií, Organizací spojených národů a Organizací pro bezpečnost a spolupráci v Evropě, což prohlubuje vzájemnou kooperaci v oblastech vzdělání, výzkumu a cvičení v boji proti kybernetickým hrozbám. NATO a jeho spojenci se snaží posílit vztahy s průmyslem a akademickou sférou, aby mohli využít inovace a držet krok s technologickým pokrokem

Jednou z výzkumných otázek je: *„Disponuje NATO orgány, které se zabývají kybernetickými hrozbami a kybernetickými útoky na členské země?“* NATO musí chránit svou síťovou infrastrukturu a k tomu jí pomáhají politické, vojenské a technické orgány, kterými jsou: Severoatlantická rada, Rada pro řízení kybernetické obrany, Centrum excelence NATO pro kybernetickou obranu, NATO Cyber Space Operations Centre a NATO Computer Incident Response Capability.

ČR reflektuje vzrůstající počet kybernetických útoků v kyberprostoru, jenž představují hrozbu pro kritickou infrastrukturu a bezpečí obyvatel. V reakci na tyto hrozby byly postupně zřízeny na území ČR instituce, které se nepřetržitě věnují ochraně a obraně kyberprostoru a zajišťují tak kybernetickou bezpečnost. Proto je jedna z částí bakalářské práce věnována popisu nejvýznamnějších českých orgánů, které se zabývají kybernetickými útoky a nabízí tak odpověď na otázku *„Jaké české orgány se zabývají kybernetickými hrozbami a kybernetickými útoky na kritickou infrastrukturu?“* K nejvýznamnějším českým orgánům, zabývajících se kybernetickými útoky patří: Národní úřad pro kybernetickou a informační bezpečnost,

Vojenské zpravodajství, Národní centrum kybernetických operací, Velitelství kybernetických a informačních operací, Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV.

NATO každoročně organizuje řadu kybernetických cvičení, kterých se účastní také zástupci z ČR, aby získali nové vědomosti a sdíleli své zkušenosti a ověřené postupy s aliančními kolegy. Tyto skutečnosti nabízí odpověď na další výzkumnou otázku *„Jakým způsobem NATO pomáhá členským zemím při budování kapacit pro kybernetickou bezpečnost?“* Nabídka kybernetických cvičení je široká a nabízí možnost procvičit se např. v hybridních, komunikačních, procesních, technických a table-top cvičeních. ČR v tomto směru nezaostává a krom toho, že je pravidelným účastníkem, bývá také v posledních letech pravidelným organizátorem.

Na základě Článku 3 Severoatlantické smlouvy je ČR zavázána udržovat a rozvíjet své schopnosti, aby zvládla odolat kybernetickým útokům. ČR disponuje klíčovými dokumenty v kybernetické obraně jako je Národní strategie kybernetické bezpečnosti ČR, Strategie kybernetické obrany ČR a Zákon o kybernetické bezpečnosti. Tyto dokumenty pomáhají ČR k dosažení cílů a splnění závazku vůči Alianci.

Cílem bakalářské práce bylo udělat průzkum stavu kybernetické obrany ČR v kontextu členství v NATO. Dalším cílem bylo prozkoumat role NATO, které sehrává v boji proti kybernetickým útokům na kritickou infrastrukturu. Oba cíle se podařilo naplnit na základě odpovědí na výzkumné otázky, které popsaly stav kybernetické obrany ČR a role NATO v boji proti kybernetickým útokům.

Pro vznik této bakalářské práce, zodpovězení výzkumných otázek a splnění cílů byla přístupná literatura dostačující, avšak při hlubším zkoumání tématu dostupnost odborné literatury, která by korespondovala s tématem práce, představovalo jeden z největších limitů. Chybí knihy a odborné články, které by se zabývaly rolemi NATO a útoky na kritickou infrastrukturu ČR. Nedostatek literatury by se mohl nahradit např. provedením interview s odborníky, kteří zkoumají NATO, anebo s pracovníky ze struktur NATO, a tím by došlo k celkovému obohacení práce. Vzhledem k malému rozsahu bakalářské práce nebylo interview provedeno, ale i přesto může tato práce sloužit jako podklad pro další podrobnější zkoumání.

Seznam literatury

Ablon, L., Binnendijk, A., Hodgson, Q. E., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. A. (2019). *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*. RAND Corporation. Dostupné z: http://www.jstor.org/stable/resrep19916

Andrle, V. (2023, 19. března). Kybernetické útoky se přesouvají z východu do zemí NATO. Důvodem je podpora Ukrajiny, míní odborník. *iROZHLAS*. Dostupné z: https://www.irozhlas.cz/veda-technologie/technologie/pribyvaji-kyberutoky-hackeri-ukrajina-rusko-cesko-nato-zpravy_2303191700_kth

Armáda České republiky. (2021, 7. října). *Velitelství informačních a kybernetických sil.* Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

BBC News. (2017, 13. května). Massive ransomware infection hits computers in 99 countries. *BBC News*. Dostupné z: https://www.bbc.com/news/technology-39901382

CCDCOE. (n.d. a). *Crossed Swords.* Dostupné z: https://ccdcoe.org/exercises/crossed-swords/

CCDCOE. (n.d. b). *Excercises.* Dostupné z: https://ccdcoe.org/exercises/

CCDCOE. (n.d. c). *Locked Shields.* Dostupné z: https://ccdcoe.org/exercises/locked-shields/

CCDCOE. (n.d. d). *North Atlantic Treaty Organisation*. Dostupné z: https://ccdcoe.org/organisations/nato/

CNN. (2023, 21. března). Russian invasion of Ukraine: A timeline of key events on the 1st anniversary of the war. *CNN*. Dostupné z: https://edition.cnn.com/interactive/2023/02/europe/russia-ukraine-war-timeline/index.html

CyCon. (n.d.). *About CyCon*. Dostupné z: https://cycon.org/

Česká televize (2013, 19. května). Kybernetičtí experti vytáhli do boje proti hackerům. *ČT24*. https://ct24.ceskatelevize.cz/ekonomika/1097776-kyberneticti-experti-vytahli-do-boje-proti-hackerum

Česká televize (2019, 23. prosince). Firma OKD zastavila těžbu, hackeři napadli její servery. *ČT24*. Dostupné z: https://ct24.ceskatelevize.cz/ekonomika/3012509-firma-okd-zastavuje-tezbu-hackeri-napadli-jeji-servery

ČTK, iDNES.cz., Kasík & Lázňovský. (2017, 14. května). Kybernetický útok zasáhl 150 zemí, experti varují před dalším atakem. *iDNES.cz*. Dostupné z: https://www.idnes.cz/technet/internet/utok-kyberneticky-europol-obeti.A170514_122739_sw_internet_ert

ČTK. (2020, 23. února). Hlavní systémy OKD jsou po loňském hackerském útoku plně funkční. Škoda přesáhne pět milionů. *iROZHLAS*. Dostupné z: https://www.irozhlas.cz/zpravy-domov/okd-hackersky-utok-virus-hacker-skoda_2002230912_ako

ČTK. (2021, 21. května). Národní knihovna ani čtyři dny po hackerském útoku není otevřená. Výpůjčky čtenářům prodlužuje. *iROZHLAS*. Dostupné z: https://www.irozhlas.cz/zpravy-domov/narodni-knihovna-hackersky-utok_2105211542_zuj

ČTK. (2022, 28. července). Hackerský útok stál ŘSD zhruba 30 milionů korun, firma chystá změny v IT. *Seznam Zprávy*. Dostupné z: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-hackersky-utok-stal-rsd-zhruba-30-milionu-korun-firma-chysta-zmeny-v-it-210170

Deines, T. M. (2023). Internationalism (politics). *Salem Press Encyclopedia.*

Disma, C. (2019). The evolving cyber warfare landscape. In M. Ozawa (Ed.), *The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges* (pp. 71–80). NATO Defense College. Dostupné z: http://www.jstor.org/stable/resrep23664.12

Beneš, V. & Císař, O. (2020). Výzkumný rámec a jeho prvky. In V. Beneš & P. Drulák. (Eds.) *Metodologie výzkumu politiky.* (s. 50–51). Slon

Ducaru, S. (2016). Is Cyber Defense Possible? *Journal of International Affairs*, *70*(1), 182–189. Dostupné z: https://www.jstor.org/stable/90012603

Emmott, R. (2018). NATO cyber command to be fully operational in 2023. *Reuters*. Dostupné z: https://www. reuters. com/article/us-nato-cyber-idUSKCN1MQ1Z9

ENISA. (n.d.). *Meeting of Central European Cyber Security Platform 2014*. Dostupné z: https://www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014

European Union Agency for Cybersecurity. (n.d. a). Cyber Europe 2022 (former CE2020). Dostupné z: https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2022

European Union Agency for Cybersecurity. (n.d. b). *ENISA supports and organises cyber exercises*. Dostupné z: https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises

Euroskop, NÚKIB, Pixabay.com & Pospíšil. P. (2022, 6. května). Čeští specialisté na kybernetickou bezpečnost uspěli v mezinárodním cvičení. *Euroskop.cz*. https://euroskop.cz/2022/05/06/cesti-specialiste-na-kybernetickou-bezpecnost-uspeli-v-mezinarodnim-cviceni/

Evropská unie. (n.d.). *Agentura EU pro kybernetickou bezpečnost*. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_cs

Goldmann, K. (2002). *The logic of internationalism: Coercion and accommodation*. Routledge.

GovCERT.Cz. (n.d.). *NCKB*. Dostupné z: https://www.govcert.cz/cs/

Horák, J. (2021, 12. března). Obecné ohrožení, vydírání a škoda 150 milionů. Vyšetřování kyberútoku míří do ciziny. *Aktuálně.cz*. Dostupné z: https://zpravy.aktualne.cz/domaci/obecne-

ohrozeni-vydirani-a-skoda-150-milionu-vysetrovani
kyb/r~6e02e8a881ad11eb89ccac1f6b220ee8/

Hromádka, M., Kko, & Malínská, E. (2016, 5. března). Seznam.cz dvě a půl hodiny nefungoval, napadli jej internetoví útočníci. *iROZHLAS*. Dostupné z: https://www.irozhlas.cz/veda-technologie_technologie/seznam-cz-dve-a-pul-hodiny-nefungoval-napadli-jej-internetovi-utocnici_201303051844_kpracharova

Hrůza, P. (2012). Kybernetická bezpečnost. *Univerzita obrany*.

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine*. NATO Defense College. Dostupné z: http://www.jstor.org/stable/resrep10354

Husák, O. (2022, 2. listopadu). Česko mohou ochromit DDoS útoky, varoval NÚKIB. *Novinky*. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-cesko-mohou-ochromit-ddos-utoky-varoval-nukib-40413303

Jiri, & Valenta, L. F. (2018). 2007: Russia's Cyber War in Estonia. In *Russia's Strategic Advantage in the Baltics: A Challenge to NATO?* (pp. 24–27). Begin-Sadat Center for Strategic Studies. Dostupné z: http://www.jstor.org/stable/resrep16828.19

Marrone, A., & Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models*. Istituto Affari Internazionali (IAI). Dostupné z: http://www.jstor.org/stable/resrep28807

Masarykova univerzita. (n.d.a). CSIRT-MU. CSIRT-MU. Dostupné z: https://csirt.muni.cz/?lang=cs

Masarykova univerzita. (n.d.b). *Cyber Czech Security Exercise | CSIRT-MU*. CSIRT-MU. Dostupné z: https://csirt.muni.cz/projects/cyber-czech

McGuinness, B. D. (2017, 27. dubna). How a cyber attack transformed Estonia. *BBC News*. Dostupné z: https://www.bbc.com/news/39655415

Národní centrum kybernetické bezpečnosti. (n.d. a). *Czech Experts on Africa Endeavor 2018*. https://www.govcert.cz/en/info/events/2641-czech-experts-on-africa-endeavor-2018/

Národní centrum kybernetické bezpečnosti. (n.d. b). *Typy cvičení*. Dostupné z: https://www.govcert.cz/cs/cviceni/typy-cviceni/

Národní centrum kybernetických operací. (2018, 6. srpna). Strategie kybernetické obrany ČR. *Národní centrum kybernetických operací*

Národný bezpečnostný úrad Slovenské republiky. *Central European Platform for Cybersecurity.* (n.d.). Dostupné z: https://www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html

NATO (2023a, 7. února). *NATO starts work on Artificial Intelligence certification standard.* Dostupné z: https://www.nato.int/cps/en/natohq/news_211498.htm

NATO Communications and Information Agency. (n.d.). *About us*. Dostupné z: https://www.ncia.nato.int/

NATO. (2018, 29. října) *Trident Juncture 2018*. Dostupné z: https://www.nato.int/cps/en/natohq/157833.htm

NATO. (2021, duben). *NATO Cyber Defence*. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

NATO. (2022, 9. září). *North Atlantic Council*. Dostupné z: https://www.nato.int/cps/en/natohq/topics_49763.htm

NATO. (2023b, 4. dubna). *NATO's response to hybrid threats.* Dostupné z: https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (n.d.a). *Cyber Coalition.* Dostupné z: https://www.act.nato.int/cyber-coalition

NATO. (n.d.b). *Cyber defence*. NATO. Dostupné z: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (n.d.c). *NATO will defend itself (Article by NATO Secretary General Jens Stoltenberg published in Prospect).* Dostupné z: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

NCKB. (n.d.). GOVCERT. Dostupné z: https://www.govcert.cz/cs/251-govcert/

NÚKIB (n.d. b). *Přínosy cvičení*. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/prinosy-cviceni/

NÚKIB. (2014, 30. května). Zpráva o stavu kybernetické bezpečnosti ČR - 2013. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2013-v4.pdf

NÚKIB. (2015, 30. května). Zpráva o stavu kybernetické bezpečnosti ČR - 2014. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2014.pdf

NÚKIB. (2016, 30. května). Zpráva o stavu kybernetické bezpečnosti ČR - 2015. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2015.pdf

NÚKIB. (2017, 30. května). Zpráva o stavu kybernetické bezpečnosti ČR - 2016. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2016.pdf

NÚKIB. (2018a, 15. srpna). Comm Czech 2018. https://nukib.cz/cs/infoservis/aktuality/1472-comm-czech-2018/

NÚKIB. (2018b, 30. května). Zpráva o stavu kybernetické bezpečnosti ČR - 2017. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2017.pdf

NÚKIB. (2020a). *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost.* Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf

NÚKIB. (2020b, 18. září). Zpráva o stavu kybernetické bezpečnosti ČR - 2019. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

NÚKIB. (2019, 30. září). Zpráva o stavu kybernetické bezpečnosti ČR - 2018. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

NÚKIB. (2020c, 2. prosince). Národní strategie kybernetické bezpečnosti. *NÚKIB.* Dostupné z: *https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf*

NÚKIB. (2021, 26. července). Zpráva o stavu kybernetické bezpečnosti ČR - 2020. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

NÚKIB. (2022a, 30. června). Zpráva o stavu kybernetické bezpečnosti ČR - 2021. *NÚKIB*. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

NÚKIB. (2022b, 6. prosince). *Experti NATO na kybernetickou bezpečnost v Estonsku pracovali na spolupráci.* https://nukib.cz/cs/infoservis/aktuality/1917-experti-nato-na-kybernetickou-bezpecnost-v-estonsku-pracovali-na-spolupraci/

NÚKIB. (n.d. a). *Kybernetická cvičení*. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/kyberneticka-cviceni/

NÚKIB. (n.d. c). *Typy cvičení.* https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/typy-cviceni/

NÚKIB. (n.d.d). *České energetické firmy čelily cvičným kybernetickým útokům.* Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1350-ceske-energeticke-firmy-celily-cvicnym-kybernetickym-utokum/

NÚKIB. (n.d.e). *Legislativa KB.* Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

NÚKIB. (n.d.f). *NÚKIB*. Dostupné z: https://www.nukib.cz/cs/o-nukib/

Policie ČR. (n.d.a). *Národní centrála proti organizovanému zločinu SKPV.* Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx

Policie ČR. (n.d.b). *Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV.* Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx

Prague Security Studies Institute. (n.d.). *PSSI NATO Summer School*. Dostupné z: https://www.pssi.cz/projects/19-pssi-nato-summer-school

Právo (2020, 13. březen). FN v Brně zažívá kybernetický útok, akutní operace se musí vozit jinam. *Novinky*. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-fakultni-nemocnice-v-brne-je-cilem-pocitacoveho-utoku-potvrdil-c-40316531

Riethofová, A. (2018, 6. srpna). Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR. *Ministerstvo obrany České republiky.* Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/

Riethofová, A. (n.d.). Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR. *Ministerstvo obrany České republiky*. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906

Samcová. J (2018, 7. listopadu). Cvičení Trident Juncture prověřilo spolupráci aliančních a partnerských států NATO při obraně napadeného území. *Armáda České republiky*. Dostupné z: https://acr.army.cz/informacni-servis/zpravodajstvi/cviceni-trident-juncture-proverilo-spolupraci-aliancnich-a-partnerskych-statu-nato-pri-obrane-napadeneho-uzemi-205189/

Shea, J. (2017). How is NATO meeting the challenge of cyberspace?. *Prism*, 7(2), 18-29. Dostupné z: https://www.jstor.org/stable/26470515

Syed, R., Khaver, A. A., & Yasin, M. (2019). CYBER WARFARE. In *Cyber Security: Where*

Does Pakistan Stand? (pp. 4–5). Sustainable Development Policy Institute. Dostupné z: http://www.jstor.org/stable/resrep24376.7

Veselá, M. (2023, 3. ledna). Zaměříme se na ochranu kritické infrastruktury státu, říká šéf elitního policejního útvaru Brejcha. *iRozhlas*.

Vojenské zpravodajství. (n.d.a). *Kybernetická obrana.* Dostupné z: https://www.vzcr.cz/kyberneticka-obrana-46

Vojenské zpravodajství. (n.d.b). *Novela zákona o vojenském zpravodajství.* Dostupné z: https://vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151

Vojenské zpravodajství. (n.d.c). *Vojenské zpravodajství*. Dostupné z: https://www.vzcr.cz/

Abstrakt

Role NATO v boji proti kybernetickým útokům na kritickou infrastrukturu České republiky

Cílem bakalářská práce je zkoumání rolí NATO v boji proti kybernetickým útokům a průzkumem stavu kybernetické obrany ČR v kontextu členství v NATO. Práce zkoumá konkrétní orgány NATO a české orgány které se zabývají kybernetickými hrozbami a kybernetickými útoky. Součástí je popis Národní strategii kybernetické bezpečnosti ČR a Strategie kybernetické obrany ČR, které prezentují vize a cíle ČR v oblasti kybernetické obrany. Práce popisuje kybernetické útoky na kritickou infrastrukturu ČR v letech 2013–2022, které vychází převážně ze zpráv o stavu kybernetické bezpečnosti ČR. Jsou představeny také typy národních a mezinárodních kybernetických cvičení. Práce používá jako metodu deskriptivní analýzu.

I přes závažnost některých kybernetických útoků, které cílily v letech 2013–2022 na kritickou infrastrukturu ČR, nedošlo k aktivaci Článku 5 Severoatlantické smlouvy. ČR pomáhají s bojem proti kybernetickým útokům české orgány. NATO nabízí možnost vzdělání v oblasti kybernetické obrany na školách NATO v Itálii a Německu, pravidelně organizuje kybernetická cvičení a disponuje orgány, které se zabývají kybernetickými útoky. ČR je na základě Článku 3 Severoatlantické smlouvy zavázána udržovat a rozvíjet své schopnosti, aby zvládla odolat kybernetickým útokům. K dodržování těchto závazků ČR pomáhají dokumenty – Národní strategie kybernetické bezpečnosti ČR a Strategie kybernetické obrany ČR.

Klíčová slova: ČR, NATO, kybernetické útoky, kybernetické hrozby, kybernetická obrana, kybernetický prostor, kritická infrastruktura

Abstract

Role of NATO in the fight against cyber attacks on the critical infrastructure of the Czech Republic

The aim of the bachelor thesis is to explore the role of NATO in the fight against cyber attacks and to investigate the state of cyber defence of the Czech Republic in the context of NATO membership. The thesis examines specific NATO and Czech authorities dealing with cyber threats and cyber-attacks. It includes a description of the National Cyber Security Strategy of the Czech Republic and the Cyber Defence Strategy of the Czech Republic, which present the vision and objectives of the Czech Republic in the field of cyber defence. The thesis describes cyber attacks on the critical infrastructure of the Czech Republic in the years 2013–2022, based mainly on reports on the state of cybersecurity in the Czech Republic. Types of national and international cyber exercises are also presented. The paper uses descriptive analysis as a method.

Despite the severity of some cyber attacks targeting the Czech Republic's critical infrastructure in 2013–2022, there was no activation of Article 5 of the North Atlantic Treaty. Czech authorities are helping the Czech Republic to combat cyber attacks. NATO offers cyber defence education at NATO schools in Italy and Germany, regularly organises cyber exercises and has bodies dealing with cyber attacks. The Czech Republic is obliged under Article 3 of the North Atlantic Treaty to maintain and develop its capabilities to resist cyber attacks. The documents - the National Cyber Security Strategy of the Czech Republic and the Cyber Defence Strategy of the Czech Republic - help the Czech Republic to comply with these commitments.

Keywords: Czech Republic, NATO, cyber attacks, cyber threats, cyber defence, cyberspace, critical infrastructure