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

Postupy krizového řízení ve vztahu k zajišťování obrany státu v kybernetickém prostoru

Crisis Management Procedures Regarding Ensuring State Defence in Cyberspace.

Bakalářská práce

Studijní program:	Ochrana obyvatelstva
Studijní obor:	Plánování a řízení krizových situací

Autor bakalářské práce:	Ondřej Bednařík
Vedoucí bakalářské práce:	Ing. Michal Kopřiva

Kladno 2021

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Bednařík**	Jméno:	**Ondřej**	Osobní číslo:	**483110**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Plánování a řízení krizových situací**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Postupy krizového řízení ve vztahu k zajišťování obrany státu v kybernetickém prostoru

Název bakalářské práce anglicky:

Crisis Management Procedures Regarding Ensuring State Defence in Cyberspace

Pokyny pro vypracování:

Předmětem práce bude provedení analýzy pojmu kybernetická obrana se zaměřením na činnosti Vojenského zpravodajství dle novely zákona 289/2005 Sb. O Vojenském zpravodajství a provedení analýzy provázání opatření krizového řízení a kybernetické obrany. V teoretické části budou rozebrány základní pojmy a bude proveden popis systému kybernetické obrany. Budou rozpracována teoretická východiska provázání kybernetické obrany a krizového řízení, které doposud nejsou stanoveny. V praktické části budou teoretická východiska provázání krizového řízení a kybernetické obrany ověřena pomocí provedení případových studií. Ty budou obsahovat krizové situace s různým stupněm intenzity kyberne-tických útoků a jejich dopadů. Závěrečná část bude věnována zpracování cílů práce, kterými je navržení opatření a postupů krizového řízení při řešení krizových situací způsobených kybernetickými útoky.

Seznam doporučené literatury:

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, Výkladový slovník kybernetické bezpečnosti: Cyber security glossary, ed. 3, Praha: Policejní akademie ČR v Praze, 2015, ISBN 978-80-7251-436-6
[2] Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Information Security Summit 2011, ed. 1, Praha: Data Security Management, 2011, ISBN 978-80-86813-22-6
[3] POLČÁK, R., Internet a proměny práva, ed. 1, Praha: AUDITORIUM, 2012, ISBN 978-80-87284-22-3

Jméno a příjmení vedoucí(ho) bakalářské práce:

Ing. Michal Kopřiva

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **15.02.2021**
Platnost zadání bakalářské práce: **18.09.2022**

doc. Mgr. Zdeněk Hon, Ph.D.
podpis vedoucí(ho) katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

14. 4. 2021
Datum převzetí zadání

Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Postupy krizového řízení ve vztahu k zajišťování obrany státu v kybernetickém prostoru vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

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

V Kladně dne 07.05.2021

…….
Ondřej Bednařík

PODĚKOVÁNÍ

Rád bych touto cestou poděkoval Ing. Michalu Kopřivovi za odborné vedení, vstřícnost a ochotu při tvorbě této práce. Zároveň bych chtěl poděkovat své rodině za podporu a trpělivost po celou dobu mého studia.

ABSTRAKT

Tato práce se zabývá bezpečností České republiky v kybernetickém prostoru se zaměřením na doplnění systému o kybernetickou obranu.

V teoretické části je proveden popis bezpečnostního systému České republiky z hlediska kybernetické bezpečnosti. Dále je provedena analýza systému kybernetické obrany se zaměřením na činnost Vojenského zpravodajství dle novely zákona č. 289/2005 Sb., o Vojenském zpravodajství.

Následně jsou rozpracovány kybernetické hrozby pro kritickou infrastrukturu a provedena analýza provázání krizového řízení a kybernetické obrany při řešení krizové situace způsobené kybernetickými útoky. Na základě této analýzy jsou navržena možná východiska, která jsou ověřena pomocí případových studií.

Klíčová slova

Kybernetická obrana; bezpečnostní systém ČR; krizové řízení; kybernetický útok; Vojenské zpravodajství

ABSTRACT

This work deals with the security of the Czech Republic in cyberspace with a focus on supplementing the system with cyber defense.

The theoretical part describes the security system of the Czech Republic from the perspective of the cyber security. Furthermore, an analysis of the cyber defense system is performed, focusing on the activities of Military Intelligence with respect to the amendment to the law No. 289/2005 Coll. on Military Intelligence.

Subsequently, cyber threats for critical infrastructure are developed and performed an analysis of the relationship between crisis management and cyber defense in solving the crisis situation, which were caused by cyber attacks. Based on this analysis, possible few optimizing proposals are suggested, which are later verified by case studies.

Keywords

Cyber Defense; Security System of the Czech Republic; Crisis Management; cyber-attack; Military Intelligence

Obsah

1 ÚVOD

Tato práce se zabývá v poslední době diskutovaným tématem, kterým je vedle kybernetické bezpečnosti právě obrana České republiky před kybernetickými útoky. Téma jsem si vybral z důvodu zájmu o tuto problematiku a právě jeho aktuálnost vzhledem k přijetí novely zákona č. 289/2005 Sb. o Vojenském zpravodajství.

Česká republika je z hlediska kybernetické bezpečnosti na vysoké úrovni a kybernetická obrana by měla cely systém doplnit a zrobustnit. Systém kybernetické obrany je tvořen řadou subjektů a jeho nedílnou součástí je na základě akčního plánu k Národní strategii kybernetické bezpečnosti pro období 2015 až 2020 schválené vládou Vojenské zpravodajství. To ke splnění tohoto úkolu zřídilo Národní centrum kybernetických operací.

Jak ukázaly nedávné kybernetické útoky na české nemocnice, hrozba kybernetických útoků už není jenom sci-fi, ale realitou i pro Českou republiku. Kyberprostor je z hlediska bezpečnosti zcela nová doména a je třeba zakomponovat tuto oblast do bezpečnostního systému České republiky potažmo postupů krizového řízení státu při řešení těchto krizových situací způsobených kybernetickými útoky.

2 CÍLE PRÁCE

Cílem práce je navržení postupů krizového řízení při řešení krizových situací spojených se zajišťováním obrany České republiky v kybernetickém prostoru a jejich ověření v rámci případových studií.

Předcházet tomu bude analýza samotné kybernetické obrany s ohledem na kompetence svěřené Vojenskému zpravodajství novelou zákona č. 289/2005 Sb. o Vojenském zpravodajství právě k podílu na zajišťování obrany České republiky. Bude provedena analýza současných postupů krizového řízení spojených se zajišťováním kybernetické bezpečnosti a jejich doplnění o prvky obrany před kybernetickými útoky.

Získané informace budou podkladem k vytvoření návrhu zapojení kybernetické obrany do postupů krizového řízení při zvládání krizových situací způsobených kybernetickými útoky a jejich ověření pomocí případových studií.

3 PŘEHLED SOUČASNÉHO STAVU

3.1 Bezpečnostní systém České republiky

V této kapitole shrnu bezpečnostní systém České republiky se zaměřením na kybernetickou bezpečnost a obranu.

Bezpečnostní systém České republiky definuje Bezpečnostní strategie České republiky jako „*komplexní hierarchicky uspořádaný bezpečnostní systém, který je propojením roviny politické (vnitřní a zahraniční), vojenské, vnitřní bezpečnosti a ochrany obyvatel, hospodářské, finanční, legislativní, právní a sociální.*“ [1]

Bezpečnostní systém ČR plní funkci nástroje při tvorbě a realizaci bezpečnostní politiky. Za zajišťování bezpečnosti státu a za řízení a funkčnost celého bezpečnostního systému ČR je odpovědná vláda jako vrcholný orgán výkonné moci. [2]

3.1.1 Prvky bezpečnostního systému ČR

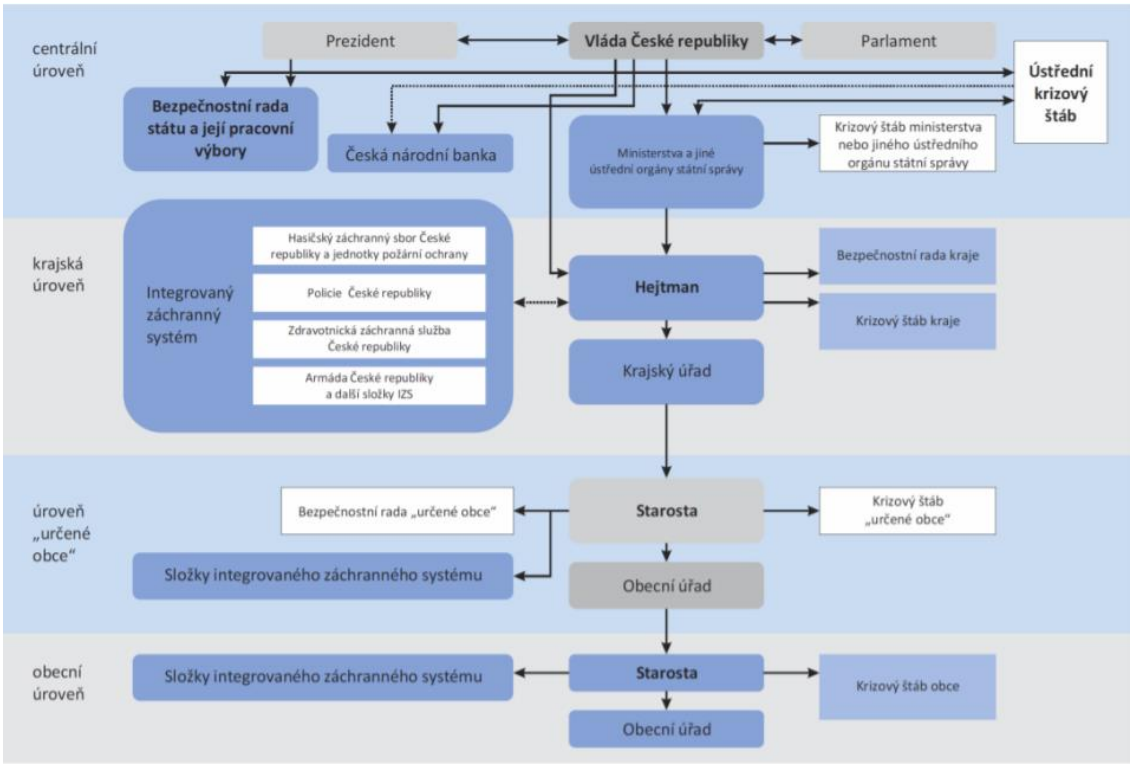
Prvky bezpečnostního systému ČR tvoří hierarchicky uspořádanou strukturu, schopnou pružně reagovat na mimořádnou událost, krizovou situaci nebo náhlou změnu bezpečnostní situace. [1]

Struktura bezpečnostního systému zahrnuje zejména:

- Prezidenta republiky
- Parlament ČR
- Vládu
- Bezpečnostní radu státu jako stálý pracovní orgán vlády
- Ústřední správní úřady
- Krajské a obecní úřady
- Ozbrojené síly
- Ozbrojené bezpečnostní sbory

- Zpravodajské služby
- Záchranné sbory a záchranné služby
- Havarijní služby [1]

Níže je uveden přehled prvků bezpečnostního systému ČR a jejich vzájemné vazby při řešení krizových situací.



Obrázek 1 - Nejdůležitější aktéři v rámci bezpečnostního systému ČR [4]

3.1.2 Bezpečnostní strategie České republiky

Klíčovým dokumentem bezpečnostního systému ČR je Bezpečnostní strategie České republiky z roku 2015, přijata usnesením vlády č. 79 ze dne 4. února 2015. Jedná se o koncepční dokument bezpečnostní politiky státu. Jejím úkolem je identifikovat zájmy České republiky, bezpečnostní rizika a hrozby z nich vyplývající. Cílem Bezpečnostní strategie ČR je zajištění systémového a koordinovaného přístupu prosazování bezpečnostních zájmů ČR a efektivní využívání mezinárodních i národních nástrojů pro účely bezpečnostní a obranné politiky. [1]

Jedná se o vládní dokument zpracovávaný ve spolupráci s Kanceláří prezidenta republiky a Parlamentem ČR. Na tvorbě se podílí i zástupci bezpečnostní komunity ČR a to jak státní tak nestátní sféry. [1]

Samotná bezpečnostní strategie zmiňuje jako jeden ze strategických zájmů zajištění kybernetické bezpečnosti a obrany ČR. Dále jsou zde uváděny důvodné obavy z růstu vojenských kapacit včetně ofenzivních kybernetických prostředků. Opomíjeno není ani uplatňování vlivových aktivit, které jsou kombinací politického, hospodářského a vojenského tlaku a dochází k nim i v kybernetickém prostoru. [1]

Bezpečnostní strategie ČR jako samostatnou hrozbu zmiňuje kybernetické útoky. Uvádí, že *„díky asymetričnosti kybernetického prostoru umožňuje státním i nestátním aktérům poškodit strategické a významné zájmy ČR bez využití konvenčních prostředků.“* [1] Poukazuje na stále se zvyšující počet a sofistikovanost kybernetických útoků zaměřených proti veřejné i soukromé sféře. Uvádí riziko významných hmotných škod způsobených kybernetickými útoky zejména na komunikační, energetické a dopravní sítě či průmyslové a finanční systémy. Opomenuta není ani úzká souvislost kybernetických útoků a politické a ekonomické špionáže. [1]

Kybernetické útoky jsou spojovány i s kritickou infrastrukturou, jejíž narušení nebo nefunkčnost může mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva nebo ekonomiku státu. [1]

V souvislosti s prevencí a potlačováním bezpečnostních hrozeb uváděné v Bezpečnostní strategie ČR, patří k prioritám vlády zajištění bezpečnosti kritické informační infrastruktury a významných informačních systémů. K tomu je určeno vládní koordinační místo pro okamžitou reakci na bezpečnostní incidenty tedy vládní CERT (Computer Emergency Response Team). V dokumentu je zmiňován Národní bezpečnostní úřad, jehož má být vládní

CERT součástí, nicméně roku 2017 roli gestora kybernetické bezpečnosti převzal nově zřízený Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který vznikl roku 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. NÚKIB bude věnována samostatná kapitola. [1] [3]

V poslední řadě Bezpečnostní strategie ČR zmiňuje podporu osvěty v oblasti kybernetické bezpečnosti vůči široké veřejnosti, jelikož právě ona může být nejzranitelnějším prvkem celého systému. [1]

3.1.3 Obranná strategie České republiky

Dalším neméně důležitým dokumentem bezpečnostního systému ČR je Obranná strategie České republiky. Jedná se o strategický dokument zpracovávaný ministerstvem obrany, navazující na Bezpečnostní strategii České republiky.

Cílem Obranné strategie ČR je vymezení přístupu vlády České republiky k zajišťování obrany České republiky a určení způsobu naplňování hlavních úkolů ozbrojených sil. [4]

Obranná strategie ČR mezi východisky obranné politiky zmiňuje používání řady nástrojů hybridní kampaně Ruskou federací vůči členským státům NATO a EU, včetně kybernetických útoků. Dále zmiňuje potencionální ohrožení bezpečnosti organizovanými kybernetickými útoky.

3.2 Kyberprostor

Vzhledem k řešené problematice je vhodné se v úvodu seznámit se samotným pojmem kyberprostor. Oproti reálnému světu je tento prostor značně specifický. Dá se říct, že je tvořen dvěma vrstvami. První vrstva je vrstva reálná tvořena jednotlivými prvky informačních a komunikačních technologií, které jsou navzájem propojené do celosvětové globální sítě. Samotný prostor mezi těmito

prvky je nehmotné médium, propojující všechny prvky do něj připojené. Kyberprostor lze definovat jako virtuální realitu bez jasně stanovených hranic, avšak závislou na technologiích nacházejících se v reálném světě. [5]

Mezi základní znaky kyberprostoru patří globálnost, decentralizace, otevřenost, bohatost na informace a interaktivnost. Z toho vyplývá, že tento celosvětový prostor, závislý na technologiích, nemá žádné hranice a obsahuje nepředstavitelné množství informací ovlivnitelných interakcí člověka. V poslední době se začíná čím dál více ukazovat, že toto virtuální prostředí může mít a má dopady i mimo kyberprostor do světa reálného.

Český Výkladový slovník kybernetické bezpečnosti definuje pojem kyberprostor jako „*Nehmotný svět informací, elektronické médium, které vzniká vzájemným propojením informačních a komunikačních systémů. Umožňuje vytvářet, uchovávat, využívat a vzájemně vyměňovat informace. Zahrnuje počítače, aplikace, databáze, procesy, pravidla, komunikační prostředky*“ popř. specificky uvádí pojem „*Český kyberprostor*“, jako „*kyberprostor pod jurisdikcí České republiky*“. [6]

Také je možné využit například znění § 2 pism. a) ZKB, kde je uvedeno, že „*kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“ [7]

Nakonec lze uvést ještě pohled České republiky prezentovaný v Bezpečnostní strategii České republiky z roku 2015, kde se uvádí že „*kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje státním i nestátním aktérům poškodit strategické a významné zájmy ČR bez využití konvenčních prostředků.*“ [1]

3.2.1 Kybernetické hrozby

Hrozbu lze definovat jako zdroje možného negativního působení, který má potenciál poškodit chráněnou hodnotu nebo aktivum. Má nežádoucí vliv na bezpečnost a může působit proti chráněným zájmům. Výkladový slovník kybernetické bezpečnosti definuje hrozbu jako *„potenciální příčinu nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace“*. [6]

Kybernetická hrozba tedy splňuje tuto definici a působí prostřednictvím kyberprostoru.

3.2.2 Kybernetické útoky

Kybernetický útok je Výkladovým slovníkem kybernetické bezpečnosti definován jako *„útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“* [6]

Bezpečnostní strategie ČR vnímá nebezpečí kybernetických útoků zejména díky jejich neustále se zvyšující sofistikovanosti a celkové četnosti jak proti veřejné tak soukromé sféře. Poukazuje na jejich možné následky zejména v komunikačních, energetických a dopravních sítích či dopravních procesech, průmyslových nebo finančních systémech a nebezpečí politické a ekonomické špionáže. [1]

Existuje mnoho způsobů dělení kybernetických útoků. Pro tuto práci rozdělíme kybernetické útoky na:

- Kybernetickou kriminalitu
- Hacktivismus
- Kybernetickou válku
- Kybernetickou špionáž

Kybernetická kriminalita

Výkladovým slovníkem kybernetické bezpečnosti je kybernetická kriminalita definována jako *„trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti"* [6]

Kybernetická bezpečnost a kybernetická kriminalita jsou jen těžko oddělitelné oblasti. Tato skutečnost je reflektována i v Rezoluci Valného shromáždění OSN ke kybernetické bezpečnosti z roku 2010, ve které je kybernetická kriminalita prezentována jako jedna z hlavních výzev kybernetické bezpečnosti. [8] Díky anonymitě kyberprostoru je to pro mnohé kriminálníky prostředí snadného finančního zisku. Boj proti kybernetické kriminalitě je rovněž součástí Národní strategie kybernetické bezpečnosti. Ta předpokládá přijetí vhodné legislativy, která by přispěla snadnějšímu prokazování kybernetické kriminality, k vytvoření vhodných technických i personálních prostředků a struktur orgánů činných v trestním řízení včetně spolupráce s ostatními subjekty v oblasti kybernetické bezpečnosti a to i v mezinárodním prostředí. [8] [9]

Hacktivismus

Hacktivismus je dle Výkladového slovníku kybernetické bezpečnosti: *„Použití hackerských dovedností a technik k dosažení politických cílů a podpoře politické ideologie."* [6] Hacktivismus je spojením slov hacker a aktivismus. Jedná se tedy o vyjádření občanského nesouhlasu nejčastěji s politickým či jiným rozhodnutím. Samotný hacktivismu je prováděn nejčastěji prostřednictvím takzvaných DDoS (Distributed Denial-of-Service) útoku na informační systémy institucí.

Jako příklad v této oblasti je možné zmínit hackerskou skupinu Anonymous která vznikla v roce 2003. Do povědomí se dostala v roce 2010 svými útoky v souvislosti s existencí serveru WikiLeaks. [10]

Kybernetická válka

Kybernetickou válku definuje slovník kybernetické bezpečnosti jako: *„Použití počítačů a internetu k vedení války v kybernetickém prostoru. Stav rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.“* [6]

Kybernetická válka představuje útok na kritické informační systémy provedený státním aktérem. Samotný pojem je součástí vojenských doktrín, takže lze předpokládat využití kybernetických schopností, při vojenských operacích. Jako první případ kybernetické války je často označována série kybernetických útoků v roce 2007 vedená suverénním státem proti Estonsku. Kybernetické útoky na webové stránky klíčových institucí, způsobili jejich několikadenní nedostupnost. Nicméně se stále vedou diskuze, zda šlo opravdu o kybernetickou válku nebo spíše kybernetický konflikt. [11]

Kybernetická špionáž

Výkladovým slovníkem kybernetické bezpečnosti je kybernetická špionáž definována následovně: *„Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy.“* [6] Dá se říci, že se jedná o klasickou špionáž, ale jsou využívána specifika kyberprostoru a možných zranitelností, které umožní útočníkům průnik do systémů a zisk citlivých dat.

3.3 Kybernetická bezpečnost

Vymezit pojem kybernetická bezpečnost může být poměrně problematické. Řada lidí se mylně domnívá, že kybernetickou bezpečností se zabývají výhradně pracovníci v informačních a komunikačních technologiích. Kybernetická bezpečnost ale zasahuje každého, kdo využívá jakékoliv prvky informačních a komunikačních systémů. Právě proto mnohdy bývá široká veřejnost nejzranitelnějším článkem systému.

Při definici kybernetické bezpečnosti budeme vycházet z již ustálených definic. Výkladový slovník kybernetické bezpečnosti uvádí, že kybernetická bezpečnost je *„souhrn právních organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* [6]

Dalším relevantním zdrojem definice kybernetické bezpečnosti je Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020. Ta uvádí, že *„kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“* [12] Kybernetickou bezpečností je běžně označována činnost při zabezpečování a ochraně vlastních systémů.

Mezi nejznámější princip kybernetické bezpečnosti patří triáda CIA. Tato triáda, vztahující se především k bezpečnosti dat a samotných informací vychází ze třech základních principů.

C – Confidentiality (důvěrnost)

I – Integrity (integrita)

A – Availability (dostupnost)

Pojem důvěrnost definuje oprávněnost přístupu subjektů (osob, entit nebo procesů) k informacím a datům. V praxi to může znamenat, že pro přístup do systému s informacemi a daty s určitým stupněm utajení má přístup pouze osoba po úspěšné autentizaci a autorizaci. [6]

Integritu dat definuje Výkladový slovník kybernetické bezpečnosti jako *„Jistotu, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.“* [6]

Dostupnost lze zjednodušeně definovat jako možnost přístupu k informacím a datům v okamžiku jejich potřeby.

3.3.1 Národní úřad pro kybernetickou a informační bezpečnost

Gestorem kybernetické bezpečnosti v České republice je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Je ústředním správním úřadem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.

Strukturu NÚKIB tvoří tři sekce:

- Sekce provozně právní
- Sekce NCKB
- Sekce informační bezpečnosti

Z hlediska kybernetické bezpečnosti je nejdůležitější sekce NCKB (Národní centrum kybernetické bezpečnosti).

Tato sekce se dále člení na:

- Odbor kybernetických bezpečnostních politik
- Odbor vládní CERT

- Odbor regulace
- Odbor kontroly

Právě odbor vládní CERT je v oblasti kybernetické bezpečnosti stěžejní. Jedná se o tzv. technickou část úřadu, která má klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů. Hlavním úkolem vládního CERTu je prvotní koordinace a řešení kybernetických bezpečnostních incidentů.

Zastoupení NÚKIB v bezpečnostním systému ČR je mimo to že jde o ústřední správní úřad také ve všech stálých pracovních výborech Bezpečnostní rady státu. Z hlediska kybernetické bezpečnosti je stěžejní Výbor pro kybernetickou bezpečnost zajišťující koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky, jejímž výkonným místopředsedou je ředitel NÚKIB, který je rovněž členem Ústředního krizového štábu.

3.3.2 Policie České republiky

Policie ČR nemá roli přímo v zajišťování kybernetické bezpečnosti. Její hlavní role je při vyšetřování kybernetické kriminality. Díky velké anonymitě kyberprostoru má velká část kybernetických útoků kriminální podtext a právě Policie ČR je orgán státu k šetření a potírání kybernetické kriminality.

Útvarem Policie ČR s působností na celém území České republiky zabývající se mimo jiné právě kybernetickou kriminalitou je Národní centrála proti organizovanému zločinu SKPV. Současně je národním kontaktním bodem pro kybernetickou kriminalitu a kontaktním místem pro počítačové hlášení závadného obsahu a závadových aktivit v síti internet. [13]

3.3.3 Zpravodajské služby

„Zpravodajské služby jsou státní orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných

ekonomických zájmů, bezpečnost a obranu České republiky." [14] Kybernetický prostor založený na informacích je zdrojem informací v této oblasti a z toho důvodu je potřeba i jejich ochrana. Může se jednat o informace, jejichž únik by mohl způsobit ohrožení zájmů České republiky. Zpravodajské služby tedy spolupracují s ostatními subjekty zajišťujícími kybernetickou bezpečnost.

3.4 Kybernetická obrana

V předchozí části jsem popsal systém zajištění kybernetické bezpečnosti ČR, jelikož provázanost kybernetické bezpečnosti a obrany je velice úzká. Robustní systém kybernetické bezpečnosti pomáhá předcházet závažným kybernetickým útokům díky zvýšení odolnosti informačních a komunikačních systémů. Pro případ selhání tohoto systému je potřeba budovat kapacity, schopné reakce na ty nejzávažnější útoky respektive kybernetickou obranu.

Samotná obrana je definována v § 2 zákona č. 222/1999 Sb. o zajišťování obrany České republiky ve znění pozdějších předpisů jako „*Souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil státu a prostředků a účast v kolektivním obranném systému."* [15]

Kybernetickou obranu definuje Výkladový slovník kybernetické bezpečnosti jako *"Obranu proti kybernetickému útoku a zmírňování jeho následků. Také rezistenci subjektu na útok a schopnost se účinně bránit."* [6]

Kybernetickou obranu lze tedy chápat jako součást bezpečnostního systému chránící zájmy státu, které jsou ohrožovány prostřednictvím kyberprostoru. Samotná obrana oproti kybernetické bezpečnosti, která pouze zodolňuje informační systémy případně detekuje kybernetické útoky, musí mít určité aktivní prvky, kterými je schopna působit proti původci kybernetického útoku.

3.4.1 Kyberprostor jako „pátá doména“

Počátek uvažování o tom že by byl kyberprostor využitelný k vojenským účelům, tedy jako pátá válečná doména byl již v 90. letech s rostoucím významem prvků komunikačních a informačních systémů a informací jako takových. [16]

Řada států již delší dobu buduje vojenské kapacity schopné působit v kyberprostoru. Jedná se o vyvíjení především kybernetických a informačních schopností. Tyto dvě oblasti jsou totiž z hlediska působení prostřednictvím kyberprostoru úzce spjaté. [16]

Ještě větší význam získal kybernetický prostor roku 2016 po summitu NATO ve Varšavě, kde byl kyberprostor uznán jako pátá válečná doména po boku dosavadních domén, kterými jsou země, moře, vzduch a vesmír. Na základě tohoto rozhodnutí NATO zahrnuje kybernetický prostor do plánování společných operací, což je samozřejmě požadováno i po všech členských státech. [17]

3.4.2 Kybernetické síly a informační operace

Jako reakce na vzrůstající hrozby v kybernetickém prostoru a uznání kybernetického prostoru jako páté válečné domény, vzniklo v roce 2017 ve struktuře armády České republiky Velitelství kybernetických sil a informačních operací VeKySIO.

Kybernetické síly a informační operace (KySIO) mohou působit samostatně, společně nebo v součinnosti s ostatními druhy sil Armády České republiky. To zahrnuje plánování a řízení operací v kybernetickém a informačním prostoru, schopnost ochrany vlastních částí kybernetického prostoru, psychologických operací a civilně vojenské spolupráce. Při vedení vojenských operací a ochraně kybernetického prostoru úzce spolupracují s Vojenským zpravodajstvím respektive Národní centrum kybernetických operací (NCKO) viz. níže. [18]

4 METODIKA

V praktické části nejdříve provedeme analýzu pojmu kybernetická obrana se zaměřením na činnost Vojenského zpravodajství při zajišťování obrany České republiky v kybernetickém prostoru. Předcházet tomu bude souhrn změn legislativy, která byla nutná k rozšíření pravomocí Vojenského zpravodajství o podíl na zajišťování obrany ČR.

Následně budou stanoveny možné kybernetické hrozby pro jednotlivá odvětví kritické infrastruktury, jejíž narušení by mohlo vést k ohrožení zájmů České republiky.

Na základě východisek teoretické části této práce a analýzy kybernetické obrany budou rozpracovány možné postupy krizového řízení při hrozbě či již probíhajícím kybernetickém útoku, který by vedl k aktivaci kybernetické obrany. Tyto postupy následně ověříme pomocí případových studií. Případové studie se budou lišit různým stupněm intenzity kybernetických útoků a jejich dopadů.

4.1 Kybernetická obrana ČR

Systém kybernetické obrany ČR je tvořen řadou subjektů a jeho nedílnou součástí se na základě akčního plánu k Národní strategii kybernetické bezpečnosti pro období 2015 až 2020 schválené vládou stalo Vojenské zpravodajství. Ke splnění tohoto úkolu vzniklo v rámci Vojenského zpravodajství Národní centrum kybernetických operací (NCKO). Dalo by se namítat, že Vojenské zpravodajství jako jedna ze tří zpravodajských služeb české republiky nemá za úkol zajišťování obrany ČR, ale získávání, shromažďování a vyhodnocování informací v oblasti obrany. Důvodem proč jako stěžejní prvek kybernetické obrany bylo vybráno právě Vojenské zpravodajství, je jednak skutečnost, že je součástí Ministerstva obrany, které ze své podstaty odpovídá za zajišťování obrany ČR a právě to, že se jedná o zpravodajskou službu. Pro úspěšnou obranu proti hrozbám z kyberprostoru je důležité právě získávání informací o těchto hrozbách, jejich původcích a taktikách.

4.1.1 Změna legislativy

Jak bylo zmíněno výše úkolem zpravodajských služeb je podle zákona č. 153/1994 Sb. o zpravodajských službách české republiky je *„získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky.“* [19] Bylo tedy nutné provést legislativní úpravy právě zákona č. 153/1994 Sb. o zpravodajských službách České republiky , ve znění pozdějších předpisů a tím rozšířit kompetence Vojenského zpravodajství o podílu na zajišťování obrany ČR v kyberprostoru.

Další nutnou změnou byla novelizace zákona č. 289/2005 Sb. o Vojenském zpravodajství. První návrh novely tohoto zákona nebyl přijat Poslaneckou sněmovnou v jejím volebním období. Projednávání tohoto návrhu vyvolávalo

značné obavy ohledně ochrany soukromí a s tím spjatou kontrolou. K diskusi byla přizvána odborná veřejnost. Na základě těchto diskuzí a pozměňovacích návrhů byl vytvořen druhý legislativní návrh, který byl počátkem roku 2019 postoupen do meziresortního připomínkového řízení.

Všechny připomínky z meziresortního řízení byly následně vypořádány a návrh byl následně počátkem roku 2020 předložen vládě. Legislativní rada vlády navrhla další dílčí změny, nicméně návrh byl přijat vládou v březnu 2020 a předložen Poslanecké sněmovně.

V 1. čtení byl návrh zákona přikázán Výboru pro obranu jako garančnímu, Stálé komisi pro kontrolu činnosti VZ a Ústavně právnímu výboru. Všechny zmíněné orgány vydali doporučující stanovisko s podmínkou přijmutí pozměňovacích návrhů. Počátkem roku 2021 prošel návrh zákona druhým čtením. Výbor pro obranu následně vydal doporučení přijmout zákon v podobě pozměňovacích návrhů. Poslaneckou sněmovnou byl návrh zákona schválen dne 12.2.2021 na hlasování č. 339 usnesení č. 1519, kde z přítomných 100 poslanců hlasovalo 72 pro a 15 proti. [20]

Senátem byl návrh zákona přijat dne 17.3.2021 usnesením č. 145, v hlasování č. 35 kde bylo 63 pro a 8 se zdrželo. [20]

Díky novele zákona č. 289/2005 Sb. o Vojenském zpravodajství získá k 1.7.2021 Vojenské zpravodajství řadu oprávnění k zajišťování obrany ČR. Jednou z nejdiskutovanějších oblastí při schvalování této novely bylo umisťování takzvaných nástrojů detekce na určených bodech veřejných komunikačních sítí. Umisťování těchto nástrojů a podmínky jejich používání zákon jasně vymezuje, včetně kontrolních mechanismů.

Dalším rozšířením kompetencí Vojenského zpravodajství je spolupráce a výměna informací jak s veřejným tak i se soukromým sektorem.

4.1.2 Úkol Vojenského zpravodajství

Jak bylo popsáno výše, obrana České republiky je úkolem Armády České republiky zejména za stavu ohrožení státu a válečného stavu. Nicméně útoky státních i nestátních aktérů prostřednictvím kyberprostoru přichází i v době míru, tedy v době kdy není vyhlášen žádný krizový stav. Díky specifičnosti kyberprostoru oproti ostatním doménám, může být samotné provedení útoku otázkou hodin nebo dokonce minut. V tomto případě je důležitá včasná detekce útoku a v případě naplnění podmínek obrany i reakce na něj. Vojenské zpravodajství resp. NCKO doplňuje systém obrany právě v této oblasti.

Podílem Vojenského zpravodajství na zajišťování obrany státu v kybernetickém prostoru je cílená detekce kybernetických útoků a hrozeb, identifikace a vyhodnocování detekovaných útoků a hrozeb a realizace opatření k jejich odvrácení.

Detekce

Právě včasné zjištění hrozby kybernetického útoku nebo samotného útoku je klíčové pro úspěšnou reakci. Je vhodné se zaměřit už na samotné vyhledávání hrozeb v kyberprostoru tzv. Cyber Threat Inteligence (CTI) v překladu zpravodajství o kybernetických hrozbách. Právě informace v této fázi jsou zásadní a to je právě jeden z důvodů svěření kybernetické obrany ČR Vojenskému zpravodajství, jakožto jedné ze zpravodajských služeb.

Dalším způsobem detekce je vyhledávání tzv. ukazatelů kybernetických útoků v samotných sítích, prostřednictví nástrojů detekce. V této oblasti se v první řadě bude jednat o spolupráci s poskytovateli zajišťujícími veřejnou komunikační síť nebo poskytujícími veřejně dostupnou službu elektronických komunikací, kteří na základě dohody budou poskytovat případné zachycení nějakého z ukazatelů kybernetického útoku vlastními nástroji detekce.

Novela zákona zákona č 289/2005 Sb. uvádí, že tyto nástroje detekce jsou umisťovány na určených místech ve veřejných komunikačních sítích a smí zaznamenávat pouze metadata pouze v rozsahu se souvisejícím s detekovaným kybernetickým útokem nebo hrozbou. Dále výslovně zakazuje jakékoliv další využití těchto nástrojů například pro odposlechy či jiné činnosti. Alternativou podle této novely je spolupráce VZ s provozovatelem veřejné komunikační sítě, který již ve své síti zřídil určitý nástroj detekce, formou dohody o poskytování metadat o kybernetickém útoku nebo hrozbě.

Tyto nástroje jsou důležitou součástí komplexního systému zajišťování obrany před kybernetickými útoky. Na základě stanovených ukazatelů kybernetických útoků budou schopné odhalit kybernetický útok, ať už jeho samotný průběh či počátek. Mohou také díky včasné detekci odhalit už přípravu kybernetického útoku, na základě čehož se přijmou opatření k jeho odvrácení.

Aktivní zásah

Jedno z nejzásadnějších oprávnění, které vojenské zpravodajství dostalo je provést aktivní zásah proti původci útoku. Novela zákona č 289/2005 Sb. nicméně jasně definuje podmínky provedení aktivního zásahu. Kybernetický útok, proti němuž je VZ oprávněno použít aktivní zásah, musí ve značném rozsahu ohrožovat důležité zájmy státu, musí být trvající nebo bezprostředně hrozící a nelze jej odvrátit v součinnosti s ozbrojenými silami České republiky a není jiné možnosti než aktivního zásahu. K takovému zásahu je VZ oprávněno pouze se souhlasem ministra obrany. [20]

Zákonem je tedy jasně stanoveno, kdy lze přistoupit k aktivnímu zásahu. Nutno podotknout, že se jedná o poslední možnost k odvrácení či minimalizování dopadu těch nejzávažnějších útoků proti zájmům chráněným státem.

Spolupráce a předávání informací

Nejzásadnější z hlediska zajišťování obrany státu v kyberprostoru je oprávnění VZ ke spolupráci a předávání informací. Novela zákona č 289/2005 Sb. uvádí několik situací možné spolupráce a výměny informací. V první řadě se jedná o již zmíněnou spolupráci při detekci kybernetických útoků a hrozeb s provozovateli veřejných komunikačních sítí.

Další a pro obranu státu před kybernetickými útoky a hrozbami velice významné je předání informace o detekovaném útoku nebo hrozbě příslušným státním orgánům k přijetí opatření. Novela se ale neomezuje pouze na příslušné státní orgány a uvádí i národní CERT a v případech hodných zvláštního zřetele další osoby, které mohou s využitím těchto informací provést opatření směřující proti kybernetickému útoku či hrozbě. [20]

Samotná spolupráce a výměna informací o možných či detekovaných kybernetických hrozbách a útocích mezi všemi subjekty zajišťujících kybernetickou bezpečnost a obranu je klíčová. Každá z institucí má ve své gesci určité nástroje k provedení opatření a tím zabránění útoku či odvrácení případné hrozby ještě než nastane. Je nutné zdůraznit, že se nejedná pouze o státní orgány, kterými jsou například NÚKIB, Policie ČR, či zpravodajské služby, ale zejména v kybernetickém prostoru i soukromé bezpečnostní společnosti či subjekty, které jsou předmětem obrany.

Neméně důležitá je i mezinárodní spolupráce se zahraničními partnery v rámci NATO (North Atlantic Treaty Organization) či EU (European Union). Zejména výměna informací o zjištěných kybernetických hrozbách a útocích, jejich analýzy a spolupráce při kolektivním zajišťování kybernetické bezpečnosti a obrany.

4.2 Odvětví KI a kybernetické hrozby

Z hlediska obrany státu je v době míru klíčová především ochrana kritické infrastruktury (KI). Dopady kybernetických útoků nemusí zůstat pouze v kybernetickém prostoru, ale mohou se projevovat tzv. kyberfyzickými účinky. Právě tyto účinky kybernetických útoků mohou mít za následek ohrožení zájmů chráněných státem a vést k zapojení aktivních prvků kybernetické obrany proti útočníkovi.

K určení kybernetických hrozeb na jednotlivé odvětví KI byla použita odvětví určená nařízením vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Tyto odvětví byla doplněna o subjekty, které sice nesplňují kritéria pro určení prvku kritické infrastruktury, ale podle vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, nebo vyhlášky č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby jsou určeni jako provozovatelé významných informačních systémů či systémů základní služby.

4.2.1 Veřejná správa

Do veřejné správy lze zařadit významné informační systémy státních institucí počínaje vládou a ministerstvy, přes veškeré úřady, systémy bezpečnostních sborů až po systémy krajů a měst. Ve veřejné správě mezi nejvýznamnější hrozby spadá narušení integrity a důvěrnosti systémů a sítí. Útočníci mohou potenciálně napadat a manipulovat s významnými informačními systémy a registry. Problémy může také způsobit nedostupnost státních systémů (např. datové schránky, finanční úřady).

4.2.2 Energetika

Oblast energetiky zahrnuje prvky výroby elektrické energie, její přenosové a distribuční soustavy, prvky pro skladování zemního plynu, přenosové a distribuční soustavy zemního plynu, distribuční soustavy ropy a prvky pro její skladování a prvky pro výrobu tepla a jeho distribuci. [21]

Tento sektor bývá vzhledem k potenciálním dopadům často označován jako jedna z nejexponovanějších a nejzranitelnějších oblastí ohroženou kybernetickými útoky. To je zapříčiněno ohromnými potenciálními ztrátami a infrastrukturními škodami, které by mohl významnější kybernetický útok napáchat. Při souhře dalších faktorů by mohl takový útok způsobit i nezanedbatelné škody na životech.

Tato oblast je často skloňována z důvodu demonstrovaných výpadků elektřiny na Ukrajině v letech 2014 a 2016, kdy v kontextu ukrajinsko-ruského konfliktu Rusové opakovaně způsobili výpadky pomocí kybernetických nástrojů v geograficky omezených oblastech. To poukazuje na nízkou odolnost energetické infrastruktury a možnost výskytu kaskádových efektů. [22]

V době míru lze pravděpodobnost kybernetického útoku na oblast energetiky považovat za hrozbu s nízkou mírou rizika. Význam této hrozby nicméně zvyšují případné následky kybernetického útoku a možnost předpřípravy prostředí již v době míru. Riziko zde nicméně představují i ransomwarové útoky, které mohou narušit fungování energetických společností.

4.2.3 Zdravotnictví

Sektor zdravotnictví zahrnuje především informační systémy nemocnic. Dále můžeme do této oblasti zařadit systémy zdravotních pojišťoven, které obsahují velké množství osobních i citlivých údajů.

V této oblasti představují největší hrozbu kybernetické útoky směřující na dostupnost a integritu zdravotnických dat. Jedná se především o ransomwarové útoky, které zašifrují systémy v nemocničních zařízeních a požadují výkupné, přičemž jsou do jeho zaplacení či do obnovy tyto systémy zašifrovány a nepoužitelné. Dopadem je potenciální nedostupnost kritických systémů či dat o pacientech.

Známý je případ takového útoku na nemocnici v Benešově v prosinci 2019, kdy byla zcela ochromena její počítačová síť včetně laboratorních přístrojů. K ještě závažnějšímu útoku došlo v březnu 2020 na Fakultní nemocnici v Brně, která díky tomu byla nucena pozastavit příjem některých nových pacientů. K poslednímu zaznamenanému útoku došlo v polovině března 2021 na tři soukromé kliniky v centru Prahy. K Podobným útokům na zdravotnická zařízení dochází například v USA, Německu či Velké Británii. Právě v Německu se pak kvůli výpadku zdravotnických služeb přičítá útoku na nemocnici v Düsseldorfu nepřímé zavinění smrti pacienta, který musel být převezen do vzdálenějšího Wuppertalu, přičemž převoz nepřežil. [23] Predikce poskytovatelů kybernetických bezpečnostních služeb na rok 2021 předpokládají další navýšení počtu těchto útoků. V roce 2020 význam hrozby rostl v souvislosti s pandemií viru COVID-19, v jejímž kontextu množství kybernetických útoků na zdravotnické systémy rostlo.

4.2.4 Finanční sektor

Do této oblasti můžeme zařadit bankovní systémy významných bank v čele s Českou národní bankou.

Finanční sektor je vedle telekomunikačních a informačních systémů jednou z oblastí s nejvyšším stupněm zabezpečení díky mnoha regulacím. Jedná se například o zákon č. 370/2017 Sb. o platebním styku, který implementoval Směrnici Evropské unie PSD2 (Payment Services Directive) o platebních službách

a provádění online plateb a nařízení komise PSD2 SCA (Payment Services Directive 2 Strong Customer Authentication) doplňující zmíněnou směrnici a požadující dvoufaktorovou autentizaci. Dále soubor mezinárodních bezpečnostních standardů PCI DSS (Payment Card Industry Data Security Standard). Cílem PCI DSS je zamezení úniku citlivých dat držitelů platebních karet a jimi provedených transakcí.

Ve finančním sektoru jsou typické útoky cílící právě na osobní data uživatelů, včetně uživatelských účtů a přístupových hesel či finančních dat. Nelze opomenout aktivity zaměřené primárně na obohacení, a to nejčastěji odcizením finančních prostředků, krádeží identity a odprodejem osobních údajů o osobách a společnostech. Mezi nejvážnější incidenty v této oblasti patří odcizení osobních údajů 145 milionů Američanů z americké finanční společnosti Equifax v roce 2017. [24]

4.2.5 Vodohospodářství

Sektor vodohospodářství zahrnuje systémy výroby a distribuce pitné vody, nebo odvádění a čištění odpadních vod. Dále systémy vodohospodářských společností zajišťující obsluhu vodních děl.

V oblasti vodohospodářství jsou bezpečnostní rizika spojena především ovládacími systémy přehrad, výrobnami pitné vody a čističkami odpadní vody. Tyto prvky jsou čím dál více digitalizovány, přičemž se při přechodu z analogových ovládacích systémů na systémy digitální často neuvažuje nad bezpečnostními aspekty. Studie A Review of Cybersecurity Incidents in the Water Sector popisuje 25 incidentů z období let 2000–2020. Zároveň poukazuje na fakt, že tento počet je pravděpodobně neúplný, jelikož celou řadu incidentů se nepodaří zachytit nebo jsou informace o nich nepublikované z důvodu udržení reputace. [25]

Riziko zde představuje především potenciálně kyberfyzická povaha útoků v tomto sektoru, neboť tato zařízení regulují např. průtok vody, kdy by vzdálená manipulace s těmito systémy mohla způsobit například záplavy, nebo její čistotu čímž by zase napadení dostupnosti či integrity systémů mohlo způsobit např. kontaminaci pitné vody.

4.2.6 Doprava

Sektor dopravy zahrnuje systémy infrastruktury silniční, železniční, letecké a lodní dopravy. Pod železniční infrastrukturu spadají systémy správy a organizace řízení železničního provozu. Letecká infrastruktura zahrnuje letiště a systémy řízení letového provozu.

V této oblasti rizika představují především útoky proti integritě dopravních systémů. Projevit se mohou regulaci dopravy na hlavních tazích a ve městech. Dále mohou ovlivnit fungování dopravních a logistických společností, logistických řetězců a mezinárodní přepravy. Možnými cíli útoků mohou být železnice, dopravní systémy měst, loděnice a přístavy, letiště a řízení letového provozu.

V červnu 2017 byly napadeny systémy dánské logistické společnosti A. P. Moller-Maersk, což narušilo logistické řetězce po celém světě a způsobilo významné prodlevy v odbavení zboží v přístavech.

4.2.7 Telekomunikační a informační systémy

Sektor komunikačních a informačních technologií zahrnuje technologické prvky pevné a mobilní sítě elektronických komunikací, datová centra, páteřní sítě a peeringové uzly.

Jak již bylo zmíněno oblast komunikačních a informačních systémů je spolu s finančním sektorem oblastí s nejvyšším stupněm zabezpečení. Jsou regulovány zejména zákonem č. 127/2005 Sb. o elektronických komunikacích a o změně

některých souvisejících zákonů a zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.

V oblasti komunikačních a informačních systémů jsou rizikem především útoky směřující na dostupnost systémů a sítí (fungování samotného systému) a důvěrnost informací. Vyloučit nelze ani přímý odposlech či útok na integritu systémů a sítí či přenášených informací. Rizikem může být i například možný přístup zadními vrátky do sítí vystavěných společností určitými společnostmi. Příkladem zde může být firma Huawei, která byla obviněna z možného uchovávání skrytého administrátorského přístupu a možnost plné kontroly nad sítí, a to potenciálně i bez vědomí operátora. Značný dopad měla také čínská špionážní kampaň „CloudHopper“, kdy útočníci pravděpodobně spjatí s čínskou civilní rozvědkou, ministerstvem státní bezpečnosti, v roce 2017 napadli poskytovatele telekomunikačních služeb v Evropě, USA a Kanadě, jižní Americe, jihovýchodní Asii a na Austrálii. Jednalo se o čím dál populárnější typ útoku na dodavatelský řetězec, tedy nikoliv přímo na cíl, ale na poskytovatele řešení, od něhož zákazník odebírá produkty a služby, jimž inherentně důvěřuje. Tím se poskytovatel stává vektorem útoku. [26] V roce 2020 poskytovatele telekomunikační služeb postihli i útoky ransomwarem, kdy se terčem útoku stal například francouzský operátor Orange.

4.2.8 Průmysl

V oblasti průmyslu jsou primárním sledovaným cílem útočníků krádeže informací a duševního vlastnictví za účelem špionáže či zpeněžení. Sekundární nebezpečí představují destruktivní útoky s potenciálem kyberfyzického účinku, případně ransomwarové útoky ochromující výrobu či obchodní činnost společností. Z hlediska obrany jsou důležité strategické a výzkumné obranné podniky. V této oblasti je třeba si adekvátně redukovat subjekty, u kterých je žádoucí, aby byly chráněny a za jakých podmínek. Míra zranitelnosti se subjekt od subjektu významně liší a nelze ji paušalizovat.

4.3 Postupy krizového řízení při kybernetickém útoku

V současnosti nejsou zatím určeny jasné postupy krizového řízení pro případ kybernetického útoku, který by svým cílem a intenzitou vedl k samotné aktivaci kybernetické obrany. Jednalo by se tedy o útok na zájmy chráněné státem a aktivnímu působení proti tomuto útoku.

4.3.1 Dosavadní postupy v rámci kybernetické bezpečnosti

Vláda ČR na základě usnesení ze dne 27. dubna 2016 č. 369 k Analýze hrozeb pro Českou republiku vydala Ministerstvu vnitra pokyn k aktualizaci Metodického pokynu ke zpracování typových plánů, které stanoví typové postupy, zásady a opatření pro řešení konkrétního druhu krizové situace identifikované v Analýze hrozeb pro Českou republiku. Tento metodický pokyn na základě Analýzy hrozeb pro ČR stanovil NBÚ (následně NÚKIB) úkol zpracovat Typový plán na krizovou situaci „Narušení bezpečnosti informací kritické informační infrastruktury“. [27] [28]

Tento typový plán na základě Metodického pokynu řeší popis krizové situace a její následky, zásady a opatření pro řešení vzniklé krizové situace. Podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti jsou subjekty podléhající tomuto zákonu povinni hlásit kybernetické bezpečnostní události a incidenty Vládnímu nebo Národnímu CERT. Pro případy těchto krizových situací (KS) typový plán uvádí, že je vhodné vyčlenit z jednotlivých krajů osobu, která v případě KS způsobené narušením kybernetické bezpečnosti KII bude schopna komunikovat s NÚKIB, správcem KII a ostatními orgány a osobami podílejícími se na řešení KS zejména s ohledem na vzájemnou výměnu informací o charakteru hrozby a existujících a potenciálních (i sekundárních) dopadech.

NÚKIB jako ústřední správní úřad pro kybernetickou bezpečnost disponuje řadou opatření k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před kybernetickými hrozbami nebo incidenty a pro řešení již probíhajících kybernetických incidentů. Těmito opatřeními jsou:

Varování

Jedná se o opatření, kterým NÚKIB upozorní subjekty podléhající ZKB tak širokou veřejnost prostřednictvím svých webových stránek. [7]

Reaktivní opatření

Tímto opatřením NÚKIB reaguje na výskyt kybernetického incidentu za účelem zmírnění jeho dopadů nebo jeho odvrácení. Obsahuje konkrétní činnosti, které má daný subjekt provést. [7]

Ochranné opatření

Toto opatření se provádí na základě zkušeností z již vyřešených bezpečnostních incidentů a jsou jím stanovena opatření ke zvýšení bezpečnosti informačních a komunikačních systémů. [7]

Stav kybernetického nebezpečí

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti tento stav definuje jako: *stav ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.* [7] Jedná se o stav, který není definovaný zákonem č. 240/2000 Sb., o krizovém řízení a jako chráněné hodnoty uvádí zájmy České republiky ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací. Těmi jsou podle tohoto zákona zachování ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního

pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.

Pravomoc vyhlásit stav kybernetického nebezpečí má ředitel NÚKIB nejdéle na 7 dní s možností prodloužení nejdéle na 30 dní. Za tohoto stavu může NÚKIB vydávat opatření i poskytovatel služby elektronických komunikací a orgánům nebo osobám zajišťujícím významnou síť což za normálního stavu nemůže. Pokud ke zvládnutí situace nepostačuje stav kybernetického nebezpečí, může ředitel NÚKIB požádat vládu o vyhlášení nouzového stavu podle zákona č. 240/2005 Sb., o krizovém řízení. [7]

Tato opatření reagují pouze na samotný kybernetický incident, nebo se snaží mu předcházet. Mimo varování se v podstatě vždy jedná o zvýšení odolnosti zranitelných míst nebo minimalizaci dopadů. NÚKIB nemá zákonné pravomoci na aktivní reakci vůči původci útoku.

Typový plán uvádí že *„dopady způsobené KS (krizovou situací) vně problematiky kybernetické bezpečnosti jsou řešeny zejména v souladu se zákonem č. 240/2000 Sb., o krizovém řízení, a zásadami řešení KS v relevantních oblastech, kde dopad nastal.“* [28]

4.3.2 Postupy krizového řízení při zajišťování kybernetické obrany

V této kapitole se pokusím navrhnout možný postup prvků krizového řízení při výskytu kybernetické hrozby či útoku, který by svojí intenzitou, původcem a cílem mohl vést až k použití aktivních prvků kybernetické obrany.

V úvodu je vhodné zmínit, že Vojenské zpravodajství na základě jemu svěřených kompetencí v první řadě doplňuje celý systém kybernetické bezpečnosti a obrany o cílenou detekcí kybernetických hrozeb a útoků, ve snaze těmto hrozbám a útokům zabránit ještě před jejich možnou realizací. Provedení aktivního zásahu je doplnění celého systému o poslední možnost zastavení či minimalizaci dopadů kybernetického útoku vůči jeho původci.

Dalším specifikem tohoto návrhu bude, že k samotnému aktivnímu zásahu by nejspíše došlo za normálního stavu, tedy bez vyhlášení krizového stavu podle zákona č. 240/2005 Sb.

Při samotném návrhu postupů krizového řízení při zajišťování obrany České republiky v kybernetickém prostoru by bylo vhodné vycházet z postupů zmíněných v předešlé kapitole. Za normálních okolností bude VZ přispívat do současného systému kybernetické bezpečnosti včasnou detekcí a předáváním informací o těchto detekovaných hrozbách s cílem jim zabránit.

Nicméně v okamžiku pozdní detekce již probíhajícího útoku, který bude splňovat zákonné podmínky k provedení aktivního zásahu, bude třeba pružné koordinace prvků krizového řízení ke zvládnutí této situace. Podle cíle kybernetického útoku by mohli hrozit kyberfyzické účinky tohoto útoku a potřeba zapojení složek integrovaného záchranného systému (IZS) do řešení krizové situace.

Podle územního rozsahu krizové situace by bylo vhodné svolat krizové štáby krajů v případě většího rozsahu Ústřední krizový štáb za účelem koordinace při řešení krizové situace způsobené kyberfyzickými účinky útoku. Součástí těchto krizových štábů by měla být osoba schopná koordinovat řešení krizové situace s NÚKIB a zasaženým subjektem, jak uvádí v Typovém plánu na krizovou situaci „Narušení bezpečnosti informací kritické informační infrastruktury“. V tomto případě by ale byla komunikace omezena pouze na ose krizový štáb kraje a NÚKIB.

Možným řešením by mohlo být zapojení Vojenského zpravodajství respektive NCKO do prvotní koordinace mezi NÚKIB a krizovým štábem kraje a následně při svolání Ústředního krizového štábu řešit krizovou situaci stávajícím systémem krizového řízení. Při tomto řešení by bylo vhodné přizvat k jednání Ústředního krizového štábu zástupce Vojenského zpravodajství respektive

NCKO, což článek 7 Statutu Ústředního krizového štábu umožňuje. [29] Tím by byla zajištěna koordinace při řešení samotného kybernetického útoku i koordinace složek IZS při řešení případných kyberfyzických účinků.

5 VÝSLEDKY

5.1 Provedení případových studií

V následujících kapitolách provedeme případové studie kybernetických útoků na různé prvky kritické infrastruktury k ověření navržených postupů krizového řízení. Tyto případové studie budou zaměřeny na různé prvky kritické infrastruktury státu a budou se lišit intenzitou kybernetických útoku a jejich dopadů. Případové studie se zakládají na reálných útocích, provedených v posledních letech na území Evropy, nicméně neuvádí konkrétní subjekty. Navržený postup krizového řízení při řešení kybernetického útoku bude ověřen v reakci těchto případových studií.

Pro lepší možnost analýzy postupů krizového řízení budou některé případové studie obsahovat několik možných variant průběhu samotného útoku a možné reakce na něj.

5.1.1 Případová studie č. 1

Tato případová studie je inspirována kybernetickými útoky na nemocnice Benešov (2019) a FN Brno (2020). [30]

Cíl útoku

Cílem kybernetického útoku je krajské nemocniční zařízení.

Typ kybernetického útoku

Jedná se o ransomwarový útok na nemocniční systémy. Útok způsobí paralyzování veškerých systémů zašifrováním veškerých dat v síti nemocnice. Může dojít k zašifrování zdravotních dat pacientů, klíčových pro jejich péči, mohou být z provozu vyřazena důležitá pracoviště jako rentgeny, magnetické rezonance nebo i celé laboratoře. Mimo útoku na dostupnost dat, může narušit

i jejich integritu a důvěrnost vzhledem Útočník kromě zašifrování data i exfiltruje a může je dále například zpeněžit, jelikož se v tomto případě jedná o vysoce citlivá osobní data pacientů.

Varianta č.1

Průběh a dopady kybernetického útoku

Po předchozí phishingové kampani byli útočníky získány přihlašovací údaje zaměstnance nemocnice. Pomocí těchto přihlašovacích údajů pronikli útočníci do systému nemocnice a následně bylo provedeno mapování sítí a úložišť nemocnice. Antivirový systém nemocnice neodhalil podezřelou aktivitu v síti. Po úspěšném zmapování sítí byl zahájen samotný proces šifrování veškerých dat nemocnice a tím způsoben naprostý kolaps nemocnice vzhledem k závislosti na těchto systémech.

Reakce na kybernetický útok

Ihned po zjištění pracovníků IT oddělení o napadení systémů kontaktovali bezpečnostního manažera nemocnice, který předal informaci členovi krizového štábu kraje určeného k zajištění koordinace při řešení krizové situace způsobené kybernetickým útokem. Následně se informace předává NÚKIB a NCKO. Hlášení tohoto útoku je i Policii ČR k zajištění důkazů k trestnímu řízení. Hejtman svolává krizový štáb kraje, který řeší strategickou úroveň koordinace. Nemocnice předává informaci krajskému operačnímu zdravotnickému operačnímu středisku o nedostupnosti poskytování zdravotní péče a nutnosti využít okolních nemocnic. Pracovníci IT oddělení nemocnice plní pokyny NÚKIB a na místo je vyslán incident response tým k asistenci při řešení útoku. NCKO v tomto případě posílá na místo také svůj tým a koordinuje činnost s NÚKIB při zajišťování stop a analýze prostředí pro následnou forenzní analýzu, díky které se pokusí zjistit šíři nákazy a indikátory kompromitace.

Použité postupy krizového řízení se zapojením kybernetické obrany

NCKO na základě předání informace o kybernetickém útoku členem krizového štábu kraje ihned zahajuje koordinaci s NÚKIB. Společným zajištěním stop a analýzou zjišťují informace k definici ukazatelů kybernetického útoku za účelem zajištění ochrany dalších subjektů před kompromitací tímto útokem včasnou detekcí.

Varianta č. 2

Průběh a dopady kybernetického útoku

V tomto případě byl k pokusu o kybernetický útok využit exploit kit (využití zranitelnosti prohlížeče) a následně zranitelnost systému využívaného nemocnicí.

Tato krajská nemocnice byla na základě analýzy určena jako důležitý objekt pro chod státu a byl zde umístěn nástroj detekce NCKO. Na základě definovaných ukazatelů kybernetických útoků (podle novely zákona č. 289/2005 Sb., o Vojenském zpravodajství) neboli indikátorů kompromitace byl tímto nástrojem detekován přístup podezřelé IP adresy. Jednalo se o IP adresu, která byla již v minulosti použita v rámci ransomwarové kampaně.

Reakce na kybernetický útok

Informace o detekované hrozbě byla ihned předána NÚKIB, který na základě svých kompetenci vydal reaktivní opatření obsahující seznam opatření k zamezení kybernetického útoku na toto nemocniční zařízení. Zároveň poskytuje metodickou pomoc a poskytuje incident response tým za účelem zastavení aktivit útočníků v jejich systémech a zamezení další kompromitace. NÚKIB zároveň vydává reaktivní opatření pro další subjekty podléhající zákonu č. 181/2014 Sb., o kybernetické bezpečnosti k provedení úkonů potřebných pro zamezení možné kompromitace. Jedná se například o provedení aktualizací,

kontrola, zda jejich systém není kompromitován a provedení bezpečnostního auditu.

Použité postupy krizového řízení se zapojením kybernetické obrany

NCKO zasazeným nástrojem detekce identifikuje kompromitaci sítě nemocnice na základě definovaných ukazatelů kybernetických útoků. Informaci ihned předává NÚKIB a zároveň předává informaci určenému členovi krizového štábu kraje. NÚKIB činí kroky ve své kompetenci za úzké koordinace s NCKO.

5.1.2 Případová studie č. 2

Tato případová studie je inspirována kybernetickými útoky na přenosovou soustavu elektrické energie na Ukrajině (2015) [22]

Cíl útoku

Cílem kybernetického útoku je přenosová soustava elektrické energie.

Typ kybernetického útoku

Jedná se o kybernetický útok pomocí malwaru, pomocí kterého útočníci získají kontrolu nad informační infrastrukturou napadeného subjektu. V tomto konkrétním případě nad řídicími systémy přenosové soustavy elektrické energie. Zmíněný malware kompromituje informační systém subjektu pomocí phishingové kampaně. Tato phishingová kampaň je založena na rozesílání e-mailů s infikovanou přílohou.

Průběh a dopady kybernetického útoku

Informační systém společnosti zajišťující provoz přenosové soustavy byl kompromitován otevřením přílohy emailu, čímž útočníci získali přístup do vnější sítě společnosti. Neodhaleni mapovali síť a možný přístup do vnitřního řídicího systému distribuční sítě neboli SCADA (Supervisory Control And Data

Acquisition). Jedná se o systém, který centrálně monitoruje průmyslová a jiná technická zařízení a procesy a umožňuje jejich ovládání. Jakmile útočníci převzali kontrolu nad řídicím systémem, spustili kybernetický útok odpojením několika rozvoden elektřiny.

Reakce na kybernetický útok

Pracovníci centrálního řídícího pracoviště ihned po zjištění výpadků předávají informaci příslušným správním úřadům a vyhlašují stav nouze. Ministerstvo průmyslu a obchodu ihned svolává krizový štáb a vzhledem k důvodnému podezření, že je krizová situace způsobena kybernetickými útoky, svolává se i Ústřední krizový štáb, kde je přizván i příslušník NCKO. Z důvodu rozsáhlých kyberfyzických účinků je vyhlášen stav nouze. Koordinací NCKO a NÚKIB a za přispění nástrojů detekce je zjištěn původ útoku v zahraničí. Jelikož kybernetický útok stále zvyšuje svoji intenzitu počtem odpojených rozvoden a tím jsou ohroženy zájmy chráněné státem a útok nelze jiným způsobem zastavit, přistoupilo NCKO k provedení aktivního zásahu proti útočící infrastruktuře. Následně byl řídicí systém odpojen od internetu a byly nasazeny incident response týmy NÚKIB a NCKO k pomoci s odstraněním malware.

Použité postupy krizového řízení se zapojením kybernetické obrany

Je svolán Ústřední krizový štáb s přizváním příslušníka NCKO. Vzhledem k rozsahu útoku a jeho dopadům je vyhlášen nouzový stav. NCKO za spolupráce s NÚKIB a výstupem detekce identifikovali útočící infrastrukturu. NCKO po splnění zákonných podmínek přistupuje k provedení aktivního zásahu za účelem zastavení kybernetického útoku.

5.1.3 Případová studie č. 3

Tato případová studie je inspirována sérií kybernetických útoků na Estonsko (2007) [11]

Cíl útoku

Cílem kybernetického útoku jsou státní instituce a finanční sektor.

Typ kybernetického útoku

Kybernetický útok je proveden pomocí tzv. DDoS útoku. Jedná se o zahlcení sítě nebo webových stránek obrovským množstvím požadavků, čímž zablokují nebo zpomalí přístup ostatním a mohou způsobit i celkový výpadek napadené sítě nebo služby případně i k jejich poškození. Je prováděn pomocí botnetů, což jsou sítě tisíců počítačů ovládaných hackery prostřednictvím škodlivého softwaru a tím zneužívaných pro páchání těchto útoků.

Průběh a dopady kybernetického útoku

Po zahájení kybernetického útoku dochází k nedostupnosti webovýh stránek vlády a některých politických stran. Zasažena jsou také zpravodajská média, díky čemuž je omezeno informování obyvatelstva o těchto útocích. Následně jsou DDoS útokem zasaženy i některé bankovní instituce a znemožněny platební operace.

Reakce na kybernetický útok

Po prvotní indikaci útoku a zjištění rozsahu je svolán Ústřední krizový štáb a přizván i zástupce NCKO. NÚKIB vyhlašuje stav kybernetického nebezpečí a úzce spolupracuje s NCKO. V rámci spolupráce při řešení kybernetického útoku jsou kontaktováni ISP (poskytovatelé internetového připojení) a peeringová centra za účelem filtrování provozu sítě a tím obranu před DDoS útokem. Po vystupňování útoku a napadení bankovních institucí se rozhoduje

o přistoupení ke krajnímu řešení tzv ostrovního provozu, kdy se část sítě se stává ostrovem bez možnosti kontaktování zvenčí, ale i naopak. Tím je zastaven kybernetický útok a následně je postupně obnovováno připojení k internetu za stálého monitoringu, že útok ustal.

Použité postupy krizového řízení se zapojením kybernetické obrany

Příslušník NCKO je přizván k řešení kybernetických útoků na jednání Ústředního krizového štábu. K řešení kybernetického předává NCKO informace ISP a peeringovým centrům podle odstavce 2 § 16f novely zákony č. 289/2005 Sb., o Vojenském zpravodajství konkrétně: *„V případech hodných zvláštního zřetele může předat informace v nezbytně nutném rozsahu také další osobě, která s jejich využitím může provést opatření směřující proti kybernetickému útoku či hrozbě.“* Následně probíhá koordinace při filtrování provozu za účelem potlačení útoky a následně přistoupení ke krajnímu řešení ostrovního provozu.

6 DISKUZE

V této práci jsem shrnul současné vnímání kybernetických hrozeb pro Českou republiku. Klíčové dokumenty bezpečnostního systému ČR, kterými jsou Bezpečnostní strategie České republiky a Obraná strategie České republiky tyto hrozby vnímají a bezpečnostní systém potažmo krizové řízení na ně reaguje řadou organizačních a procesních opatření.

K zajištění kybernetické bezpečnosti byl zřízen Národní úřad pro kybernetickou a informační bezpečnost, který zajišťuje odolnost kritických a významných informačních systémů vůči kybernetickým útokům a hrozbám. Na zajišťování kybernetické bezpečnosti se podílí i řada dalších institucí. Vedle Policie ČR řešící trestně právní rovinu kybernetické bezpečnosti také všechny zpravodajské služby České republiky v mezích své působnosti.

Tento systém kybernetické bezpečnosti bylo nutné doplnit o možnost aktivního působení proti zdroji útoku i za stavu míru. Tento úkol byl svěřen Vojenskému zpravodajství. K plnění tohoto úkoly byla nutná změna legislativy. Jednak k samotné účasti Vojenského zpravodajství na zajišťování obrany České republiky a zároveň svěření pravomocí k výkonu tohoto úkolu.

Analýzou obrany České republiky před kybernetickými útoky a působností Vojenského zpravodajství při jejím zajišťování na základě novely zákona č. 289/2005 Sb., o Vojenském zpravodajství byli podrobněji popsány kompetence a postupy při zajišťování kybernetické obrany.

Jedná se především o cílenou detekci kybernetických hrozeb a útoků, možnost provedení aktivního zásahu při těch nejzávažnějších útocích a spolupráce s ostatními institucemi zajišťujícími kybernetickou bezpečnost z veřejné i soukromé sféry.

Následně bylo vzhledem k těmto novým kompetencím Vojenského zpravodajství navrženo možné začlenění kybernetické obrany do současného systému kybernetické bezpečnosti vzhledem k řešení krizových situací, tedy do krizového řízení.

Tento návrh počítá s již zavedenými postupy na základě Typového plánu na krizovou situaci „Narušení bezpečnosti informací kritické informační infrastruktury“, který vytvořil NÚKIB na základě Analýzy hrozeb pro Českou republiku. Tento typový plán počítá s určením osoby na krajské úrovni, která by při KS způsobené narušením bezpečnosti KII koordinovala a komunikovalas NÚKIB, správcem KII a ostatními orgány zapojenými do řešení KS.

Návrh postupů krizového řízení počítá s tím, že by tato určená osoby byla součástí krizového štábu kraje a při řešení KS by vedle NÚKIB úzce komunikovala i s NCKO. Tyto dvě instituce by samozřejmě také úzce spolupracovali a každá z nich by k řešení KS podnikala kroky ve své působnosti.

Pro případ rozsáhlých kybernetických útoků, nebo útoků s déletrvajícími následky je součástí návrhu rovněž přizvání zástupce Vojenského zpravodajství resp. NCKO k jednání Ústředního krizového štábu. Statut Ústředního krizového štábu takové řešení umožňuje. Tím by byla zajištěna koordinace při řešení samotného kybernetického útoku i koordinace složek IZS při řešení případných kyberfyzických účinků.

Tento návrh postupů krizového řízení při řešení kybernetických útoků byl ověřen provedenými případovými studiemi, které se zakládali na již provedených útocích v posledních letech v rámci Evropy.

Ukázalo se, že NCKO po účinnosti novely zákona č. 289/2005 Sb., o Vojenském zpravodajství bude schopno doplnit systém kybernetické bezpečnosti o detekci ukazatelů kybernetických útoků. Ta přispěje nejen k detekci již probíhajícího kybernetického útoku, ale i včasnému odhalení útoku ve fázi přípravy. Nedílnou

součástí detekce bude i tzv. CTI, které na základě sběru informací o kybernetických hrozbách, útocích, taktikách a samotných aktérech doplní již zmíněné ukazatele kybernetických útoků.

Případové studie ukázali, že i předávání informací a spolupráce se soukromým sektorem, kterou umožní novela zákona č. 289/2005 Sb., o Vojenském zpravodajství pomůže řešit kybernetické útoky a v mnohých případech jim i předcházet.

Je třeba zdůraznit, že v současnosti je oblast kybernetické obrany vytvářena i ostatními státy. Nejsou tedy dostatečné zkušenosti, z kterých by se dalo vycházet. Ukáže nejbližší doba, zda jsou současná nastavení postupů účinná pro řešení těch nejzávažnějších kybernetických útoků.

7 ZÁVĚR

Tato práce byla zaměřena na vznikající oblast bezpečnostního systému ČR, kterou je zajištění obrany České republiky v kybernetickém prostoru. Doplnění současného systému kybernetické bezpečnosti o pravomoci Vojenského zpravodajství zajistí větší bezpečnost a suverenitu České republiky.

V práci byly navrženy možné postupy zapojení kybernetické obrany do krizového řízení ověřené případovými studiemi. Tyto postupy se snaží nastínit zapojení Vojenského zpravodajství resp. NCKO, které rozšiřuje možnosti a kompetence bezpečnostních složek při řešení kybernetických útoků.

Zapojení Vojenského zpravodajství do zcela nové a pro zpravodajskou službu specifické role obrany České republiky v kybernetickém prostoru, která by mohla působit i mimo krizové stavy, je pro bezpečnostní systém ČR zcela novým nástrojem, který bude muset být reflektován v dosavadním systému.

Jelikož se jedná o novou oblast, bude v blízké budoucnosti určitě stále rozvíjena a aktualizována na základě získaných zkušeností. Bude velice zajímavé sledovat tento vývoj a případně se na něj zaměřit při zpracování diplomové práce.

8 SEZNAM POUŽITÝCH ZKRATEK

CERT	Computer Emergency Response Team
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NATO	North Atlantic Treaty Organization
EU	European Union
ZKB	Zákon o kybernetické bezpečnosti
OSN	Organizace spojených národů
DDoS	Distributed Denial-of-Service
CIA	Confidentiality, integrity, availability
NCKB	Národní centrum kybernetické bezpečnosti
SKPV	Skupina kriminální polici a vyšetřování
VeKySIO	Velitelství kybernetických sil a informačních operací
NCKO	Národní centrum kybernetických operací
VZ	Vojenské zpravodajství
CTI	Cyber Threat Inteligence
KI	Kritická infrastruktura
PSD	Payment Services Directive

PSD SCA	Payment Services Directive 2 Strong Customer Authentication
PCI DSS	Payment Card Industry Data Security Standard
KII	Kritická informační infrastruktura
KS	Krizová situace
IZS	Integrovaný záchranný systém
SCADA	(Supervisory Control And Data Acquisition)

9 SEZNAM POUŽITÉ LITERATURY

[1] *Bezpečnostní strategie České republiky 2015* [online]. Praha: Ministerstvo zahraničních věcí ČR, 2015 [cit. 2021-03-29]. ISBN 978-80-7441-005-5. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[2] *TERMINOLOGICKÝ SLOVNÍK POJMŮ Z OBLASTI KRIZOVÉHO ŘÍZENÍ, OCHRANY OBYVATELSTVA, ENVIRONMENTÁLNÍ BEZPEČNOSTI A PLÁNOVÁNÍ OBRANY STÁTU* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2021-03-30]. Dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

[3] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

[4] *Obranná strategie České republiky* [online]. Praha, 2017 [cit. 2021-04-01]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/obranna-strategie-2017.pdf

[5] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.

[6] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 1. oficiální vyd. Praha: Policejní akademie ČR v Praze, 2012. ISBN 978-80-7251-378-9.

[7] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. *Zákony pro lidi* [online]. [cit. 2021-03-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181/zneni-20200201

[8] *Rezoluce Valného shormáždění OSN ze dne 17. března 2010 (64/211) „Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures“* [online]. [cit. 2021-04-17]. Dostupné z: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

[9] *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online]. Praha: NÚKIB, 2020 [cit. 2021-03-31]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[10] *Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous* [online]. 2015 [cit. 2021-05-09]. Dostupné z: https://academic.oup.com/jhrp/article/7/3/391/2412155

[11] *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective* [online]. [cit. 2021-05-10]. Dostupné z: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[12] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020* [online]. Praha: NBÚ, 2015 [cit. 2021-03-31]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf

[13] *Národní centrála proti organizovanému zločinu SKPV* [online]. [cit. 2021-05-09]. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx

[14] *Zákon č. 153/1994 Sb. Zákon o zpravodajských službách České republiky* [online]. [cit. 2021-05-11]. Dostupné z: https://www.zakonyprolidi.cz/cs/1994-153

[15] Zákon č. 222/1999 Sb. Zákon o zajišťování obrany České republiky. *Zákony pro lidi* [online]. [cit. 2021-04-01].

[16] BASTL, Martin a Zuzana GRUBEROVÁ. Cyberspace as a "Fifth Domain"?. *Vojenské rozhledy* [online]. 2013, **22**(4), 10-21 [cit. 2021-03-08]. ISSN 12103292. Dostupné z: doi:10.3849/2336-2995.22.2013.04.010-021

[17] *Warsaw Summit Communiqué* [online]. 2016 [cit. 2021-05-09]. Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[18] *Velitelství kybernetických sil a informačních operací* [online]. [cit. 2021-04-25]. Dostupné z: https://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

[19] POKORNÝ, Ladislav. *Zákon o zpravodajských službách České republiky: Zákon o Bezpečnostní informační službě ; Zákon o Vojenském zpravodajství : komentář*. Vydání první. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7552-378-5.

[20] *Sbírka zákonů č. 150 / 2021* [online]. 2021 [cit. 2021-04-22]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39112

[21] *Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury* [online]. 2010 [cit. 2021-05-09]. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432

[22] *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid* [online]. 2016 [cit. 2021-05-09]. Dostupné z: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[23] *The untold story of a cyberattack, a hospital and a dying woman* [online]. [cit. 2021-05-05]. Dostupné z: https://www.wired.co.uk/article/ransomware-hospital-death-germany

[24] *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.* [online]. 2017 [cit. 2021-04-01]. Dostupné z: https://epic.org/privacy/data-breach/equifax/

[25] *A Review of Cybersecurity Incidents in the Water Sector* [online]. Journal of Environmental Engineering 146, 2020 [cit. 2021-04-03]. Dostupné z: https://arxiv.org/pdf/2001.11144.pdf

[26] *Operation Cloud Hopper: What You Need to Know* [online]. 2017 [cit. 2021-04-17]. Dostupné z: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know

[27] *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 27. dubna 2016 č. 369: k Analýze hrozeb pro Českou republiku* [online]. 2016 [cit. 2021-04-27]. Dostupné z: http://www.hzscr.cz/soubor/uv-369-analyza-hrozeb-pdf.aspx

[28] *Typový plán: Narušení bezpečnosti informací kritické informační infrastruktury* [online]. NÚKIB, 2019 [cit. 2021-04-27]. Dostupné z: https://www.hzscr.cz/soubor/635-priloha-c4-pdf.aspx

[29] *Statut Ústředního krizového štábu* [online]. [cit. 2021-05-09]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/pracovni-vybory/ustredni-krizovy-stab/statut-UKS.pdf

[30] *Analýza hrozby ransomware* [online]. 2020 [cit. 2021-05-10]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

10 SEZNAM POUŽITÝCH OBRÁZKŮ