POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Kyberterorismus, kybernetická válka – prostředky, metody a protiopatření

Diplomová práce

Cyberterrorism, cyber warfare – resources, methods and countermeasures
Master thesis

VEDOUCÍ PRÁCE
PhDr. Mgr. Eliška Jonášová, Ph.D.

AUTOR PRÁCE
Bc. Andriana HALAI

PRAHA
2022

Čestné prohlášení

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

V Praze, dne 03. 03. 2022

Bc. Andriana HALAI

Poděkování

Tímto bych chtěla poděkovat vedoucí své diplomové práce PhDr. Mgr. Elišce Jonášové, Ph. D za to, že mi umožnila tuto práci pod její odborným vedením sepsat a dále též děkuji za její přístup, pomoc a cenné rady.

Poděkování patří taktéž mé rodině a přátelům za jejich morální podporu.

ANOTACE
Diplomová práce se zabývá problematikou kyberterorismu, jeho charakteristikou a současnými projevy v mezích kyberprostoru, včetně kybernetické války. Obsahově se práce skládá z teoretické a praktické části. V úvodu je obecně vymezena problematika terorismu a jeho historie, následně je popsána charakteristika kyberterorismu, kde jsou uvedeny jeho metody a prostředky útoků. Další kapitola se zaměřuje na charakteristiku legislativního zajištění kybernetické bezpečnosti a v závěru teoretické části je vymezena teorie kybernetické války. Z praktické části je pak patrné, že kyberterorismus je rychle šířící se odvětví konvenčního terorismu a kybernetické útoky jsou reálnou hrozbou pro vládní systémy, které s postupem času a rozvojem technologií budou ještě více umocňovány.

KLÍČOVÁ SLOVA
terorismus * kyberterorismus * kyberprostor * kybernetická válka * kybernetický útok * metody kyberterorismu * bezpečnostní hrozba * kybernetická bezpečnost

ANNOTATION
The thesis deals with the issue of cyberterrorism, its characteristics and current manifestations within the confines of cyberspace, including cyberwarfare. The content of the thesis consists of theoretical and practical parts. In the introduction, the issue of terrorism and its history is generally defined, followed by the characteristics of cyberterrorism, where its methods and means of attacks are described. The next chapter focuses on the characteristics of the legislative provision of cyber security, and the theoretical part concludes by defining the theory of cyber warfare. The practical section then shows that cyber terrorism is a rapidly spreading branch of conventional terrorism and cyber-attacks are a real threat to government systems that will only become more acute as time passes and technology advances.

KEYWORDS
terrorism * cyberterrorism * cyberspace * cyberwarfare * cyberattack *cyberterrorism methods * security threat * cybersecurity

Obsah

Cíle a metodika práce 11
Teoretická část 12
1.Terorismus 13
1.1 Vymezení pojmů 13
1.2 Historie a vývoj terorismu 15
1.3 Typologie a metody terorismu 17
1.3.1 Typy terorismu 17
1.3.2 Metody terorismu 19
1.4 Terorismus a kyberprostor 20
2. Kybernetický terorismus 21
2.1 Kyberterorismus jako bezpečnostní hrozba 21
2.2 Kybernetické metody 24
2.3 Kybernetické útoky a jejich výskyt 27
2.4 Charakteristika kybernetických útočníků 33
3. Koncept kybernetické bezpečnosti 35
3.1 Systém zajišťování kybernetické bezpečnosti v ČR 36
3.2 Základní dokumentace v oblasti kybernetické bezpečnosti 37
3.3 Legislativní zajištění bezpečnosti kyberprostoru v ČR 37
3.4 Odpovědné instituce a orgány v oblasti kyberterorismu 38
3.5 Úroveň kybernetické bezpečností České republiky 41
3.6 Opatření k řešení výzev a hrozeb v oblasti kybernetické bezpečnosti 42
4. Fenomén kybernetické války 44
4.1 Vymezení pojmu kybernetická válka 44
4.2 Prostředky kybernetického boje 47
4.3 Obrana proti kybernetickým hrozbám 48
Praktická část 51
5. Řízený strukturovaný rozhovor s odborníky na dané téma 52
5.1 Metodologie výzkumů 52
5.2 Cíle 52
5.3 Otázky pro rozhovor a jejích stručná charakteristika 53
5.4 Vyhodnoceni rozhovoru s pracovníkem Oddělení informačních systémů a komunikačních technologií, Útvaru policejního vzdělaní a služební přípravy Policie České republiky 54

5.5 Vyhodnoceni rozhovoru s odborníkem v oblastí ochrany utajovaných informací (OUI) 58
6. Výsledky, které byly zjištěny řízeným strukturovaným rozhovorem 59
6.1 SWOT analýza 59
Závěr 62
Seznam literatury 64
Seznam příloh 71
Příloha 1 72
Příloha 2 76

Seznam zkratek

AFCEA – Armed Forces Communications & Electronics Association

AČR – Armáda České republiky

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

ČR – Česká republika

Dos/DDos – Daniel of Service/Distributed Daniel of Service

EU – Evropská unie

GRU – Hlavní správa rozvědky

GŠ AČR – Generální štáb Armády České republiky

ICT – Informační a komunikační technologie

IP – Internet Protocol

ISIS – Islámský stát

IT – Informační technologie

IZS – Integrovaný záchranný systém

MO – Ministerstvo obrany

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NATO – Severoatlantická aliance

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

NCKO – Národní centrum kybernetických operací

NCOZ – Národní centrála proti organizovanému zločinu

NCSI – Network Connectivity Status Indicator

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OPIS – Operační a informační střediska

OUI – Ochrana utajovaných informací

PČR – Policie České republiky

SKPV – Služba kriminální policie a vyšetřování

SZBP – Společná zahraniční a bezpečnostní politika

TČ – Trestný čin

USA – Spojené státy americké

VeKySIO – Velitelství kybernetických sil a informačních operací

ÚZSI – Úřad pro zahraniční styky a informace

VZ – Vojenské zpravodajství

ZKB – Zákon o kybernetické bezpečnosti

ZS – Zpravodajská služba

Úvod

Současná vývojová fáze společnosti je charakterizována postupujícím technologickým a vědeckým pokrokem. Informační a komunikační technologie jsou jedním z nejdůležitějších faktorů ovlivňujících život společnosti v 21. století. Jejich revoluční dopad se týká způsobu života lidí, jejich vzdělávání a práce, interakce vlády a občanů.

Informační a komunikační technologie se rychle staly důležitým stimulem pro rozvoj světového společenství. Zároveň je vývoj vědeckého a technologického pokroku vždy doprovázen výbuchem i negativních sociálních projevů. Tomuto nasvědčuje skutečnost, že virtuální svět se stal novým prostředím pro páchaní různého druhu ilegálních jednáni. Zároveň proces informačního rozvoje přináší hrozby ze strany destabilizujících politických sil, které využívají tyto technologie ke zločinným účelům. Nejzávažnější hrozbu v této souvislosti představují kyberterorismus a kybernetická válka, poněkud zvaná i hybridní válkou. Ve většině případů je zastupují teroristické organizace, které využívají informační a komunikační systémy pro plánovaní a organizování rozsáhlých kybernetických útoků v rámci kyberprostoru.

Kyberterorismus je mnohostranný fenomén, který je do značné míry způsoben nekontrolovaným využíváním globálních sítí, nedostatečnou pozorností ze strany státu a zpravodajských služeb k této problematice, který se projevuje útoky na počítače, počítačové programy a sítě nebo informace v nich, s cílem vytvořit ve společnosti atmosféru strachu a beznaděje za účelem dosažení cílů a zájmů teroristických aktérů, což vyžaduje, aby světové společenství spojilo své síly k účinnému boji proti němu. Otázky spojené s kybernetickou bezpečností a globálním využívaním internetu jsou v současné době na vrcholu seznamu výzev v oblasti mezinárodní bezpečnosti. Současná situace vyžaduje urychlený vývoj účinných mechanismů pro prevenci a potlačení teroristického chování v kyberprostoru.

Bohužel, v dnešní době zkušenosti světového společenství nedostačují k tomu, aby této hrozbě plně čelilo. Toto přímo souvisí se skutečností, že kyberterorismus je nadnárodní fenomén a jeho účastníci jsou schopni ohrozit informační systémy

odkudkoli na světě. Koneckonců díky globální síti internetu mohou kyberteroristé shromažďovat podrobné informace o cílech svých útoků a jejich přesné poloze. Hlavní vlastností, která poskytuje nejširší spektrum možností na internetu je anonymita. Předvídat nebo včasně odhalit hrozící kybernetický útok je velice složité. V rámci kyberprostoru je také možné získat finanční podporu různých teroristických akcí, což se ve většině případů odehrává v souvislostí s kybernetickou válkou, kde útočníkům přispívá politický systém nepřítele.

Prevence kyberterorismu je složitým procesem, protože tento jev má mnoho politických, sociálních, ekonomických, historických, psychologických a dalších příčin. Tyto příčiny by proto měly být předmětem neustálé pozornosti a preventivních zásahů ze strany státu a společnosti. Regulace informační sféry v moderní demokratické společnosti je složitým a nejednoznačným úkolem. Hlavním problémem je zde potřeba zachovat demokratické principy svobody informací spolu se zavedením určitých omezení jejich šíření v zájmu národní bezpečnosti.

Úspěšné potlačení kyberterorismu závisí do značné míry na důkladném teoretickém pochopení problému. Zájem badatelů problematiky kyberterorismu a formy jeho projevů je dán změnou politické a bezpečnostní situace ve světě, zejména aktuálního vojenského konfliktu Ukrajiny a Ruské federace, zvýšenou aktivitou teroristických organizací na mezinárodní scéně, nutností spojit úsilí veřejných a státních institucí, orgánů činných v trestním řízení, všech konstruktivních sil různých politických orientací na národní i globální úrovni v boji proti tomuto fenoménu, kde se informace přirovnává ke zbrani.

Cíle a metodika práce

Cílem diplomové práce je: prozkoumat prioritní oblastí kyberterorismu a kybernetické války, rozebrat koncept kybernetické bezpečnosti České republiky, možné vzniky bezpečnostních hrozeb a rizik v souvislostí s kybernetickými útoky, zmínit se o prevenci a opatřeních, kterými disponuje Česká republika proti tomuto typu terorismu.

Práce si klade za cíl probrat základní charakteristiku kyberterorismu a kybernetické války, která se odehrává ve virtuálním světě, konceptu kybernetické bezpečnosti České republiky, možného vzniku bezpečnostních hrozeb v souvislostí s kybernetickými útoky a jejich eliminaci.

Pro dosažení hlavního cíle a náplně práce jsem zvolila pro teoretickou část následující metody: pozorováni, vědecký popis, explanaci a analýzu. Pomocí vybraných metod se pokusím systematizovat vědecké přístupy ke studiu kyberterorismu, vymezit hlavní pojmy v souvislostí s touto problematikou a identifikovat politické, sociální, ekonomické a další příčiny kybernetických útoků a také popsat specifické rysy a trendy v dané oblastí činnosti. V rámci analytické metody rozeberu zkušenosti České republiky s kybernetickými incidenty a určím jejích význam pro rozvoj v dané problematice.

Metodologie a cíle praktické časti práce budou podrobněji popsány v odpovídajícím oddílu.

Teoretická část

1.Terorismus

Každé období dějin lidstva má svá specifika a s ním je spjata jak řada výhod, tak i značné množství problémů. Některé lidé dobře zvládají, jiné naopak zaznamenávají velký růst. Jedním z takových problémů je terorismus, který prošel obrovským vývojem a v dnešní době se stal globální hrozbou pro lidstvo. Globální povahu má zejména proto, že nerespektuje žádné geografické a politické hranice, vzbuzuje a šíří strach spolu s nejistotou mezi obyvatelstvem mnoha států. Vyznačuje se prudce zvýšeným technickým vybavením, vysokou úrovní organizace a dostupností velmi významných finančních prostředků.

1.1 Vymezení pojmů

K získání představy o tomto jevu a pro pochopení dalších souvislostí a bezpečnostních aspektů, které terorismus přináší, je nutné nejdřív objasnit podstatu pojmu, neboť pojmové projasnění představuje základní východisko pro další úvahu. Slovo terorismus má svůj původ z latinského terror (strach**,** hrůza, zděšení, bázeň) nebo terreo (třást se, strašit, nahánět strach). Jeho hlavními vlastnostmi je tedy nahánět nebo šířit strach, jde o násilné zastrašování. Za teroristické činy označujeme činy nebo události, které lze pochopit jako činnost nebo akce. Za akci terorismus si označují sami teroristé, kdy Carlos Marighella, který se honosil přezdívkou „otec městského terorismu“, definoval terorismus jako akci.[1]

Terorismus a s ním spojené bezpečnostní problémy je zapotřebí vnímat komplexně a s multioborovým přístupem. Vědecká komunita a akademická sféra zde sehrávají nezastupitelnou úlohu.

Jedním z nejpodstatnějších výzkumů je správné vymezení tohoto pojmu. Tento fenomén je používán jako pojem akademický, úřední, právní a také obecný, proto je terorismus velice složitým pojmem, neexistuje, ale definicie, na které by se shodlo více osob. Zkoumat se ho snažila spousta odborníků, ale každý z nich má

[1] BRZYBOHATÝ, Marian. *Terorismus I*. Praha: Police History, 1999. ISBN 80-902670-1-7.

jinou představu.[2] Neuzavřená definice terorismu způsobuje značné problémy zejména při vědeckém vymezení pojmu a jeho následném využití pro výzkum a vědu.

Jak jsem již uvedla výše, terorismus nelze přesně definovat, jde o neuzavřený pojem. Přesto se řada odborníků shodla alespoň na primárním základu.

Po událostech 11. září 2001 se muselo reagovat na definici teroristického činu, která byla zveřejněna dne 27. prosince 2001 Radou EU v dokumentu pod názvem „Společný postoj Rady EU pro užití zvláštních opatření pro boj s terorismem“, 2001/931/SZBP. Zde teroristický skutek je chápán jako množina vyjmenovaných činů, které mohou svou podstatou vážně ohrozit obyvatelstvo, chod konkrétního státu nebo mezinárodní organizaci.[3]

V roce 1980 v USA byla vyvinuta definice terorismu, kterou můžeme přijmout za výchozí pro posuzování a hodnocení teroristických činů: *“Terorismus je propočítané použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen”.*[4]

Pro Českou republiku je významnou definice, založená na skutkové podstatě trestného činu, „teroristicky útok“ uvedena v § 311 z. 40/2009 Sb. trestního zákoníku. Podmínkou každého teroristického útoku je právě co největší reakce lidí a médií, čím více lidí je ovlivněno a zaujato, tím větší úspěch má celá operace. K tomu teroristé využívají všechny dostupné prostředky, virtuální prostředí internetu, sociálních sítí, ovšem výjimkou nejsou ani tištěné materiály, které jsou integrální součástí propagandy. Terorismus 21. století a s ním spojené násilí destabilizuje demokratické základy státu tím, že živí pochybnosti o funkčnosti systému

[2] MAREŠ, Miroslav. *Terorismus v ČR.* 1.vyd. Brno: Centrum strategických studií, 2005. ISBN 80-903333-8-9.
[3] Terorismus a měkké çíle: Definice terorismu. *Ministerstvo vnitra České republiky* [online]. [cit. 25.10. 2021]. Dostupné z: https://www.mvcr.cz/cthh/clanek/definice-terorismu.aspx
[4] BRZYBOHATÝ, Marian. *Terorismus I.* Praha: Police History, 1999. ISBN 80-902670-1-7.

samotného. Cíleně infikuje obyvatelstvo a jeho nejvíce ovlivnitelné segmenty ideologickými a náboženskými doktrínami, které legitimizují násilí. Násilné útoky inspirované politickými či náboženskými motivy vždy probouzejí dostatek nespokojenců. Násilí patří mezi hlavni nástroje terorismu a je mocným způsobem, který ovlivňuje psychiku a emoce lidi ohrožených terorismem.[5]
V určitých částech definice jsou odlišné, ale skoro ve všech se objevuje zastrašení obyvatelstva, a to hrozbou nebo užitím násilí proti nezúčastněným osobám.

1.2 Historie a vývoj terorismu

Jakýkoli společenský jev se vyskytuje na pozadí určitých okolností. A čím je tento fenomén pro společnost složitější a závažnější, tím hlubší musí být pohled na okolnosti, které jej způsobily. Nárůst násilí v každodenním životě moderní společnosti nás nutí obracet se k teoretickým a psychologickým počátkům terorismu, jehož kořeny sahají do staletí.

První projevy terorismu byly zaznamenány již ve starověku. Historiografie této problematiky je velmi rozsáhlá, proto se v kontextu mé práce zastavíme u nejznámějších příběhů vzniku a vývoje terorismu, vzhledem k tomu, že tento fenomén je nejen historicky dostatečně dlouhý, ale také prošel určitým vývojem. Potvrzení o starobylosti terorismu a existenci teroristických organizací nalézají někteří odborníci dokonce v bibli, přičemž za příklad prvních teroristických činů považují tresty seslané Bohem na Egypt. Před více než dvěma a půl tisíci lety bylo na území Egypta po dobu téměř tří měsíců prováděno deset teroristických útoků, nazývaných „egyptské tresty“[6], během nichž probíhaly biologické, ekologické, chemické útoky. Bylo to provedeno za účelem zastrašení faraona, který držel židovské etnikum v otroctví, ale pro obyvatelstvo Egypta to také bylo velkým utrpením.

První, koho považujeme za teroristy, byla židovská nábožensko-politická skupina zealotů-sikariů. Informace o teroristických aktivitách sikariů jsou vzácné a protichůdné. Zealotové-sikariové vraždili svými dýkami Římany, kteří okupovali část

[5] VEGRICHTOVÁ, Barbora. *Hrozba radikalizace: terorismus, varovné signály a ochrana společnosti*. Praha: Grada, 2019. ISBN 978-802-7120-314.
[6] Starý zákon, Exodus 5:12.

Blízkého východu. Je také známo, že židovský národ bojoval nejen proti římské kolonizaci, ale i proti svým sousedům. O tom, že skupina sikariů byla teroristická, svědčí jejich neobvyklá taktika zabíjení – denní světlo, přítomnost veřejnosti a dýka. Často jsou tyto metody připisované k dnešnímu terorismu. Teroristické činy pod jejich vedením sledovaly sobecké i politické cíle.

Současně v mnoha zemích existovaly další skupiny, zejména v Indii byly Thugové. Oni patřili do indické hinduistické sekty vyznavačů bohyně Kálí a hlavní náplní víry bylo vraždění. Činnost se datuje od 7. do poloviny 19. století. Skupiny fungovaly velmi organizovaně a své krutosti páchaly nenápadně. Mezi jejich oběti patřily především cestovatelé, obchodníci a karavany. Thugové své působení ukončili již v 90. letech 19. století, když se Indie stala součástí Britského impéria.

Ještě jednou významnou skupinou raného terorismu byli asasíni nebo „zdrogování zabijáci“. Hlásili se k větvi šíitského islámu. Slovo asasín vzniklo z výrazu haša-šíjún. Historici došli závěru, že jejich charakteristickým znakem bylo, že před samotným výkonem Asasíni užívali hašiš. Akce Asasínů byly různého charakteru a měly světské a náboženské cíle.

První zkušenost s revolučním masovým terorem je spojena s významnou událostí historií – Velkou francouzskou revolucí, která razantně ovlivnila vývoj terorismu. Zda se, že většího počtu vražd v tak krátkém časovém úseku se ve světových dějinách hledá těžko. Dá se to pouze přirovnat k Bartolomějské noci, kdy během několika hodin bylo z náboženských důvodů zavražděno obrovské množství hugenotů. Na konci XVIII. a během dvou třetin XIX. století pojem „teror“ byl vnímán v nejširším smyslu neoddělitelném od jeho etymologie. Toto slovo bylo používáno k popisu jak otevřené násilné formy diktatury, tak praxe jednorázových politických vražd. Terorismus moderní éry začíná v polovině minulého století spolu s rozkvětem anarchismu. Evropa bojovala a snažila se svrhnout stávající monarchistický režim, který byl považovaný za dost nespravedlivý vůči dělnické třídě. V Rusku vznikala různá hnutí, která měla za cíl svrhnout cara. Anarchisté si uvědomili, jak je důležitá publicita a tím pádem vraždily veřejně.

Jednou z nejvýznamnějších ruských teroristických akcí byl pokus o atentát na cara Alexandra II. v roce 1881, kterým po několikerých neúspěšných se podařilo dokončit vraždu. Svého vrcholu anarchismus dosáhl v roce 1890, a to především ve Francii, Itálii, Španělsku a Spojených státech. V tomto období vznikly významné teroristické atentáty. Například v roce 1914 atentát v Sarajevu, kdy byl zabit arcivévoda František Ferdinand a jeho manželka Žofie Chotková. Tento útok měl za následek rozpoutání 1. světové války. Z toho je patrné, že když teroristický útok je dobře naplánován a proveden, může mít velký vliv na společnost, ba dokonce iniciovat události, které mohou změnit historický vývoj v celosvětovém měřítku.

Praktiky terorismu prošly dynamickým evolučním vývojem, a to zejména od sedmdesátých let 20. století po současnost, a to ve dvou klíčových aspektech, ve volbě cíle útoku a ve způsobu jeho provedení.[7]

Dnešní terorismus je problémem nejen zemí s politickými, národnostními či náboženskými nepokoji, ale i celého společenství. Moderní terorismus prokázal možnost zranit značné množství lidí a zničit obrovské množství věci bez použití tradičních zbraní.

1.3 Typologie a metody terorismu

1.3.1 Typy terorismu

Výjimečná rozmanitost typů a projevů terorismu v moderním světě, rozdíly, které existují v jeho povaze, směru a účelu, ve vědeckých kruzích, vyvolávají řadu snah o zpracováni jeho typologie. Jedním z nejobtížnějších problémů je stanovení výchozích parametrů a kritérií, kterými by se mohl řídit vývoj jednotného scénáře moderního terorismu, neboť určují jeho ideologický a politický obraz. Vzhledem k neutralitě lze za nejpropracovanější považovat problematiku klasifikace různých typů teroristických činů, která našla své praktické uplatnění při přijetí několika mezinárodních úmluv o boji proti různým formám terorismu, o nichž bude řeč později.

[7] VEGRICHTOVÁ, Barbora. *Hrozba radikalizace: terorismus, varovné signály a ochrana společnosti*. Praha: Grada, 2019. ISBN 978-802-7120-314.

Jak už bylo zmíněno v mojí práce, určité typy terorismu mají mezi sebou velmi nepatrné hranice. Charakteristické znaky jednoho typu často se mohou objevit i jako znaky jiného druhu. Tomuto problému lze zabránit, pokud lze u určitého druhu terorismu včas rozpoznat motivace (jaké daná skupina má zaměření) a cil teroristů (čeho chtějí dosáhnout). Od tohoto propojení se proto odvíjí i základní členění typologie terorismu. V základu terorismus rozdělujeme na:

- kriminální
- patologický (psychopatický)
- politický (ideologický).

Hlavním účelem kriminálního terorismu je dosaženi příslušného zisku, u patologického typu jsou akce primárně provedené kvůli psychickému sebeuspokojení jedince a terorismus politický nehledá žádnou přímou materiální výhodu, ale je zaměřen na určitou kolektivní myšlenku. Politický, resp. ideologický terorismus, lze dále členit na:

- ultralevicový
- ultrapravicový
- etnický
- náboženský
- environmentální
- vigilantistický (jedna se o sjednávaní pořádku)
- „single-issue“ (hnutí proti potratům)
- kybernetický.

Vedle typologie uvedené výše, rozlisujeme kategorie domácího a mezinárodního terorismu související s počtem zemí, v nichž terorismus působí.[8] Domácí neboli vnitrostátní terorismus působí v rámci jednoho státu a dotýká se jeho bezpečnostních zájmů. Mezinárodni terorismus se dotýká bezpečnostních zájmů více států.

[8] Terorismus: Typologie terorismu. *Ministerstvo vnitra České republiky* [online]. [cit. 01.11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d

1.3.2 Metody terorismu

Vzhledem k tomu, že terorismus prošel obrovským vývojem, můžeme ho rozdělit do různých forem a metod páchaní. Formy neboli metody terorismu jsou závislé na rozvoji doby a spolu s tím na prostředcích, které jsou přístupné pro teroristy. Mezi typické vlastnosti teroristických metod patří nebezpečnost, bezohlednost a také brutalita. Čím větší je brutalita, rozsah teroristického útoku a následky, tím pravděpodobněji na ně bude upřena pozornost medií, která rychle, bohužel ne vždy zcela pravdivě, informují veřejnost o různých událostech. Rozpoutají co nejvíce publicity, strachu a ohrožení u co největšího okruhu lidí. Teroristé si vybírají takové metody, které budou vyvolávat maximální psychologicky efekt. Na pozadí následného hromadného napětí společnosti, frustrace a deprivace jsou realizovány psychologické manipulace a operace, jejichž účelem je dosažení teroristických cílů.[9] V tomto lze terorismus považovat za mimořádně ostrou formu psychologické války.

V dnešním světě teroristé mají ke své dispozici plné vybavení nejmodernějšími zbraněmi, od klasických forem až k virtuálnímu prostředí. Formy terorismu lze rozdělit na klasické teroristické metody a na moderní metody, které přímo souvisí s technologiemi a stručně budou uvedeny. K tzv. „klasickým“ teroristickým metodám patří:

- střelba, použití sečných a bodných zbrani, ubití
- výbuchy pum samy o sobě
- výbuchy, které jsou iniciátory další ničivé činnosti
- únosy, braní rukojmích
- násilí na turistech
- dopisní bomby
- specifické cíle postmaterialistického a environmentálního teroru.[10]

[9] BRZYBOHATÝ, Marian, et al. *Terorismus a my: Základy sebeobrany*. 1. vyd. Praha: Computer Press, 2001. ISBN 80-7226-584-9.
[10] Terorismus: Klasické teroristické metody. *Ministerstvo vnitra České republiky* [online]. [cit. 01. 11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d

Nové technologie, možnosti využiti počítačů a další pronikavý rozvoj vědy a techniky vytváří podmínky pro urychlení výzkumu a vývoje. Jsou už vytvořeny předpoklady k tomu, že výsledky vědeckých pokusů mohou být zneužity i pro teroristické cíle. Proto k „moderním“ teroristickým metodám řadíme:

- jaderné technologie
- biologické technologie
- chemické technologie
- zvukové zbraně
- kyberterorismus.[11]

Nyní bych ráda věnovala svoji pozornost problematice kyberterorismu, která se vyvíjí zřejmě dynamičtěji něž většina jiných výzkumných priorit.

1.4 Terorismus a kyberprostor

Fenomény současného světa s velmi rostoucím významem – internet, infomační a telekomunikační sítě a technologie pronikly do všech oblastí lidského života, což znamená do našich každodenních činností. Inovace umožnily člověku a jeho pracovní stránce zdokonalení, ale čím více se konkrétní technologie stávají nezbytnou součástí života jedince a společnosti, tím více se zvyšuje frekvence a dopady jejich zneužití. Tyto dopady a změny nám umožnily poznat novou podobu světa – tzv. kyberprostor neboli všudypřítomný svět informací.

Pojmem kyberprostor je označován prostor kybernetických aktivit či prostor vytvořený ICT, který vytváří svět virtuální reality, ve které dochází ke spojeni fyzického světa se světem kybernetickým.[12] Tak vznikla tzv. informační společnost, která se pohybuje v tomto prostoru a je definována takto: *„Společnost, kde kvalita života i perspektiva sociálních změn a ekonomického rozvoje závisí na informacích*

[11] Terorismus: Moderní teroristické metody. *Ministerstvo vnitra České republiky* [online]. [cit. 01. 11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d

[12] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

a schopnosti jejich využití, tj. informace se stává klíčovým faktorem takovéto společnosti“. [13]

Jak jsem již uvedla, kyberprostor čelí určitým hrozbám, které jsou spojené se zneužitím informací, zničením jich, či dokonce vyřazením z provozu. Jednou z takových hrozeb je kyberterorismus. Nebezpečí práce ve virtuálním světě se zvyšuje s nárůstem ukládání dat a se vzrůstající uživatelskou náklonností k internetu. V dnešní době před hrozbami v kyberprostoru není chráněn žádný stát, Česká republika nevyjímaje. Navíc, zhoršení bezpečnostní situací ve světě zvyšuje nároky na schopnost samostatně reagovat na bezpečnostní hrozby vznikající v kyberprostoru.[14]

2. Kybernetický terorismus

Ve věku rostoucích online útoků a různých teroristických aktivit se vyvíjely i podoby a formy terorismu. Kybernetický terorismus byl objasněn v 80. letech minulého století, kdy termín vytvořil vedoucí pracovník Institutu pro bezpečnost a zpravodajství (ang. Institute for Security and Inteligence) Barry Collin, který poukázal na to, že jak fyzický, tak virtuální svět se začaly prolínat a přetvářet do nějaké konkrétní formy terorismu.[15] Z toho vyplývá, že kyberprostor a jeho nástroje se začaly využívat k teroristickým účelům.

2.1 Kyberterorismus jako bezpečnostní hrozba

V českém prostředí definice kyberterorismu zatím neexistuje a vzhledem k tomu NBU vytvořil pro potřeby Auditu národní bezpečnosti zcela novou definici, která zni takto: *„Kyberterorismus zahrnuje agresivní a excesivní jednání, které je*

---

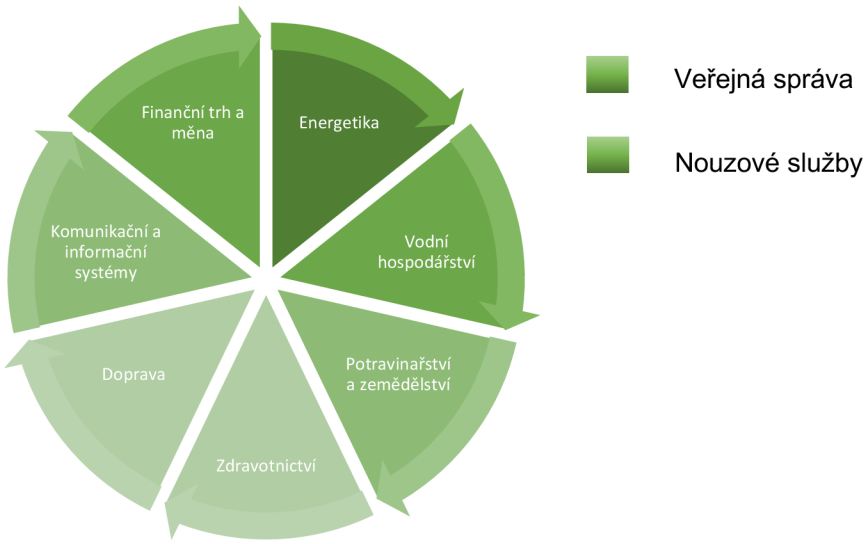
[13] JANOUŠEK, Michal. *Kyberterorismus: terorismus informační společnosti* [online]. [cit. 01.11. 2021]. Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html

[14] Audit národní bezpečnosti: Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR. Hrozby v kyberprostoru. *Ministerstvo vnitra České republiky* [online]. Praha, 2016. [cit. 15. 11. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[15] COLLIN, Barry. Future of Cyberterrorism: The physical and virtual worlds converge. *Crime and Justice International Volume: 13 Issue: 2* [online]. 1997. [cit. 15. 11. 2021]. Dostupné z: https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge

prováděno se záměrem vyvolat strach ve společnosti a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožujících chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy".[16]

Ještě jednou z nejvíce používaných definic kyberterorismu, je definice Dorothy E. Denningové. Podle jejích slov kybernetický terorismus je navržen tak, aby zastrašil i donutil řídicí mechanismus státu a obyvatele k plnění určitých politických nebo společenských akcí. Bereme to jako útoky proti počítačovým sítím a kritické infrastruktury, které by měly vyústit v násilí na osobách či majetku, nebo přinejmenším způsobit vážné škody.[17] Kritickou infrastrukturou se rozumí takové systémy, kdy narušeni jejich funkce by vedly k zásadním ekonomickým, obranným, politickým a sociálním důsledkům. Dle nařízení vlády 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury, pak prvky KI se dělí do devíti oblastí:

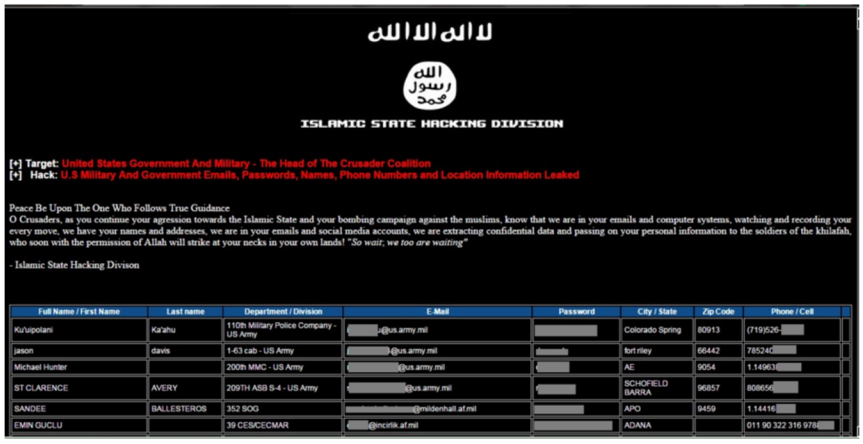


Graf 1 Odvětvová kritéria pro určení prvku kritické infrastruktury – sestavila autorka

[16] Audit národní bezpečnosti: Třídění hrozeb. *Ministerstvo vnitra České republiky* [online]. Praha, 2016. [cit. 15. 11. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[17] DENNING, Dorothy E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* [online]. 1999. [cit. 15. 11. 2021]. Dostupné z: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

S definicemi Collina a Denningové, a tedy i základními charakteristikami kyberterorismu, se ztotožnila řada dalších autorů. Kyberterorismus zahrnuje plánované útoky proti informacím, informačním systémům, počítačovým programům a datům, jejichž výsledkem je násilí proti civilnímu obyvatelstvu. Je třeba také zdůraznit, že primárním cílem kybernetického terorismu není nutně zničení, dezintegrace neboli dezinformace objektů v kyberprostoru, ale může být využito určitých serverů k zesílení dopadu jiných fyzických hrozeb.[18] Více něž polovina ze 79 hlavních teroristických skupin, které jsou na seznamu MZV USA má na internetu vlastní stránky.[19] Teroristé používají šifrované E-maily k plánovaní vlastních operací a šíří na internetu vlastní propagandu včetně dětské ve formě různých her a pohádek.[20] Většinou se jedná o různé zprávy, videa, nahrávky, elektronické časopisy, kde jsou vysvětlené ideologické postoje a praktická činnost spojena s teroristickými aktivitami. Například lze zmínit praxi organizace tzv. Islámský stát (ISIS). Ten v nebývalé míře využívá internet a různé sociální sítě k propagandě a rekrutaci nových členů, také prostřednictvím internetu řídí činnost svých partnerů v zahraničí.


لا اله الا الله

ISLAMIC STATE HACKING DIVISION

[+] Target: United States Government And Military - The Head of The Crusader Coalition
[+] Hack: U.S Military And Government Emails, Passwords, Names, Phone Numbers and Location Information Leaked

Peace Be Upon The One Who Follows True Guidance
O Crusaders, as you continue your agression towards the Islamic State and your bombing campaign against the muslims, know that we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khalafah, who soon with the permission of Allah will strike at your necks in your own lands! *"So wait; we too are waiting"*

- Islamic State Hacking Divison

Full Name / First Name	Last name	Department / Division	E-Mail	Password	City / State	Zip Code	Phone / Cell
Ku'uipolani	Ka'ahu	110th Military Police Company - US Army	[redacted]@us.army.mil	[redacted]	Colorado Spring	80913	(719)526-[redacted]
jason	davis	1-63 cab - US Army	[redacted]@us.army.mil	[redacted]	fort riley	66442	785240[redacted]
Michael Hunter		200th MMC - US Army	[redacted]@us.army.mil	[redacted]	AE	9054	1.14963[redacted]
ST CLARENCE	AVERY	209TH ASB S-4 - US Army	[redacted]@us.army.mil	[redacted]	SCHOFIELD BARRA	96857	808656[redacted]
SANDEE	BALLESTEROS	352 SOG	[redacted]@mildenhall.af.mil	[redacted]	APO	9459	1.14416[redacted]
EMIN GUCLU		39 CES/CECMAR	[redacted]@incirlik.af.mil	[redacted]	ADANA		011 90 322 316 978[redacted]

Obr. 1 Hackování zveřejněné Islámským státem (ISIS) [21]

[18] GORDON, Sarah. *Cyberterrorism* [online]. Symantec Security Response. 2003 [cit. 15. 11. 2021]. Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.7114&rep=rep1&type=pdf
[19] *Terrorist Designations and State Sponsors of Terrorism: Foreign Terrorist Organizations* [online]. U.S. Department of state [cit. 15. 11. 2021]. Dostupné z: https://www.state.gov/foreign-terrorist-organizations/
[20] *Al-Fateh – The Hamas Web Magazine for Children: Indoctrination to Jihad, Annihilation and Self-Destruction* [online]. Institute for Monitoring Peace and Cultural Tolerance in School Education, 2009. [cit. 15. 11. 2021]. Dostupné z: https://www.impact-se.org/wp-content/uploads/2016/04/Al-Fateh_Report_2009_final.pdf
[21] Islamic State Hacking Division. DBpedia [online]. [cit. 15. 11. 2021]. Dostupné z: https://dbpedia.org/page/Islamic_State_Hacking_Division#

Teroristická propaganda je dost nežádoucím jevem, jelikož může mít obrovský vliv na celou řadu posluchačů a sympatizantů a v důsledku toho i popuzovat k teroristickému činu.

Švédský profesor a zástupce ředitele švédské agentury pro výzkum v oblasti obrany Roland Heickerö kyberterorismus a jeho dopady popsal takto: *„Internet umožňuje působit anonymně za předpokladu, že uživatelé mají potřebné znalosti a dovednosti jak se vyhnout digitálnímu sledovaní a forenzním vyšetřovatelům v oblasti počítačové techniky…řízený a kvalifikovaný kybernetický útok na kritické infomační systémy by mohl mít velký vliv na společnost a mohl by tak v závislosti na tom, jaký systém je napaden, způsobit ztráty na životech“.* [22] Tato definice poukazuje na závislost mezi jednotlivými aktéry terorismu a jejich možností v rámci kyberprostoru.

Je třeba si také uvědomit, že ne ve všech případech zůstává využíváni kyberprostoru zcela anonymní. Útoky na strategické průmyslové, vojenské a vládni cíle jsou velmi náročné na realizaci, protože aktivní budovaní sil státních protiteroristických struktur, zvyšování úrovně jejich technického vybaveni a zlepšování operační metody a činnosti mohou vest k vysledování iniciátorů kybernetického útoku.[23] Většinou nejdůležitější systémy jsou chráněny formou „air-gap“, což znamená, že zařízení jsou oddělena od internetu nebo od firemních sítí.

2.2 Kybernetické metody

Z výše popsaných definic je tedy možné shrnout základní charakteristické znaky kyberterorismu:

- politická motivovanost
- násilí, psychologicky efekt překračující okruh přímých oběti či svědků útoku

[22] HEICKERÖ, Roland. *Terrorism online and the change of modus operandi* [online]. Command and Control Research Program (U.S.), 2008. [cit. 15. 11. 2021]. Dostupné z: http://dodccrp.org/events/13th_iccrts_2008/CD/html/papers/209.pdf

[23] DRMOLA, Jakub. Konceptualizace kyberterorismu. Vojenské rozhledy. Praha: Ministerstvo obrany České republiky [online]. 2013, č. 2 [cit. 16. 11. 2021]. ISSN 1210-3292. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/konceptualizace-kyberterorismu

- útoky na důležité informační infrastruktury.

V závislosti na následném využití kyberprostoru terorismem, lze kyberterorismus dělit na dva směry:

- propagandistický (informační)
- přímý.

Propagandistický neboli informační terorismus, tedy takový, jehož podstatou je negativní či odmítavá reakce na aktuální stav politické nebo mezinárodní situace. Sem patří i výše zmíněná propagace teroristických skupin, které ke své činnosti využívají kyberprostor. Druhou skupinou je kyberterorismus přímý, kde se realizuje přímé napadení určitých cílů, popřípadě i jejich likvidace. Závisí to na zkušenostech a možnostech uživatelé síťových služeb a IT specialistů. [24]

Vzhledem k obrovskému rozvoji informačních a komunikačních technologií jsou i různé taktiky a metody kyberterorismu. Mezi základní taktiky patři:

- použití technologie jako součást tradičních metod
- čistý kybernetický útok využívající výhradně komputerovou technologií.[25]

Metody kyberterorismu jsou založeny především na zneužití integrity počítačových systémů. Základnými programovými prostředky využívající komputerovou technologií jsou tzv. malware. Termín je kombinací dvou slov – malicious, což znamená škodlivý a software. Jde o programové vybavení, jehož funkcí je narušení a infiltrace jednotlivých prvků sítě a služeb. Nejčastěji se jedná o neoprávněné využiti dat uživatele a ovlivňovaní chodu nějakého systému. Do této kategorie spadají různé počítačové viry, adware a spyware, souhrnně nazývané škodlivé kódy. V další části práce charakterizuji jednotlivé druhy malware.

---

[24] JANOUŠEK, Michal. *Kyberterorismus: terorismus informační společnosti* [online]. [cit. 16.11. 2021]. Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html

[25] BRZYBOHATÝ, Marian. Cyberterorismus [online]. [cit. 16.11. 2021]. Dostupné z: https://docs.google.com/presentation/d/0B9UHcDuG1unoZ1I3eGU4RDNLcVU/edit?resourcekey=0-vHiXohR0KyqEk_OkgZKFWw#slide=id.p1

Virus – je samostatný škodlivý program, který se sám dokáže reprodukovat, může být napojen i na jiné programy nebo dokumenty, infikuje počítač a jeho soubory s cílem získat kontrolu nad zařízením a ukrást citlivá data. Jeho účelem je degradace operačních systémů s využitím paměti a diskové kapacity.

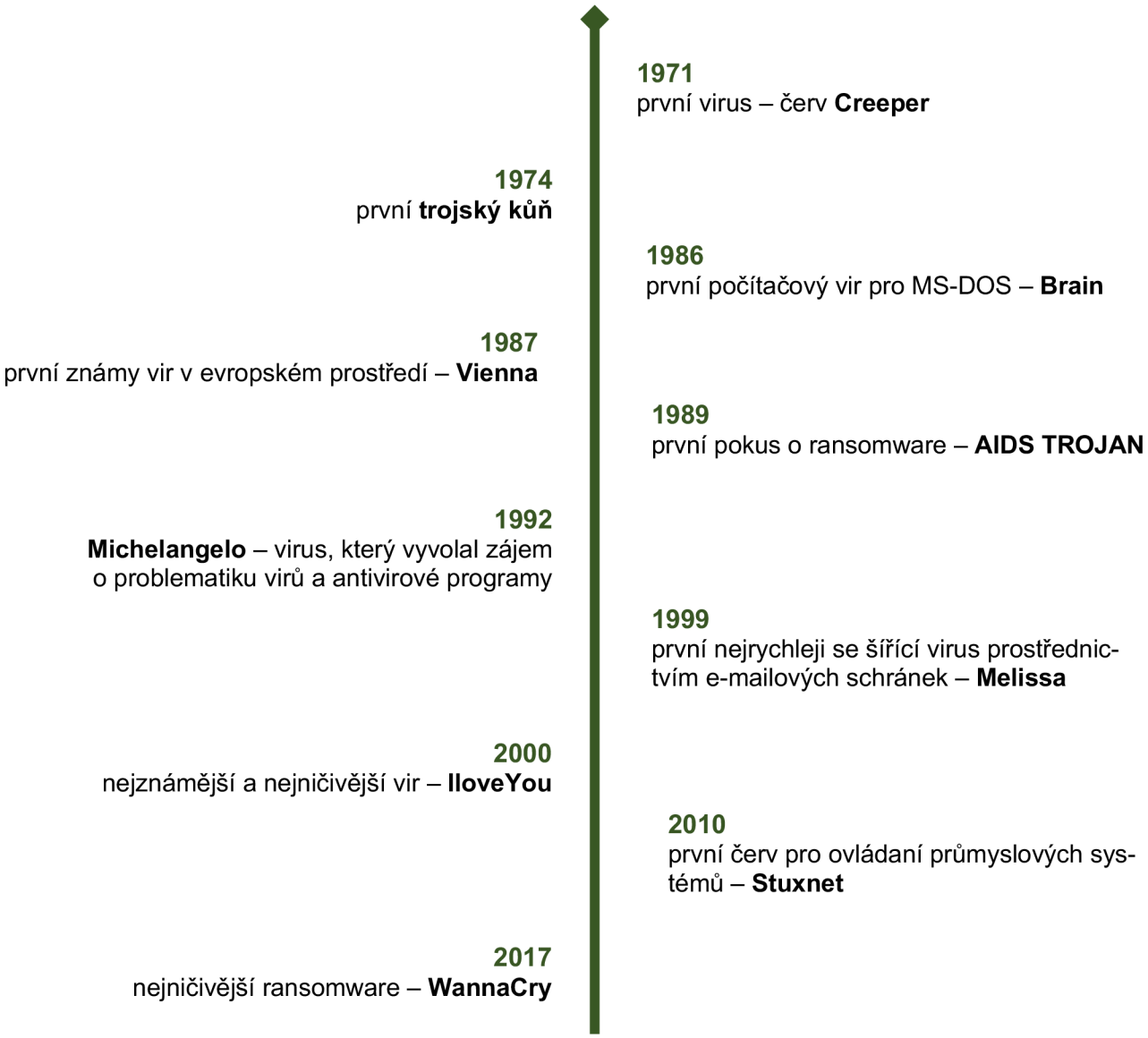


Schéma 1 Chronologie nejznámějších typu virů [26] – sestavila autorka

Adware – je typ malwaru, který se může ukrývat v počítači nebo mobilním telefonu, „odposlouchává“ data svých uživatelů, sleduje jejich internetové aktivity, aby mohl

[26] *Co je počítačový virus + druhy virů: Kdy vznikly viry a jak na ně vyzrát?* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/virus/

lépe cílit obsah vyskakovacích reklam. Sám o sobě je neškodný, může ale odkazovat na phishingové stránky.[27]

Spyware – je škodlivý sledovací program. Neoprávněně se instaluje do počítače, tajně shromažďuje data o počítačů, chování uživatele a následně je odesílá svému tvůrci, který tyto informace prodává nebo využívá k útoku. Spyware je těžko odhalitelný a skrývá svou činnost za důvěryhodně vypadající procesy.[28]

Na základě výše popsaných prostředků se může zdát, že kyberterorismus ohrožuje pouze kyberprostor a dotýká se pouze technologií. Ve skutečnosti to není tak. Nesmíme ale zapomenout na to, že důsledkem útoku v rámci kyberprostoru může být jak fyzická likvidace, tak i poškození majetku nebo systému, což může vést k velkým ztrátám na životech. Kupříkladu počítačový červ Stuxnet cílem, jakého byla jaderná elektrárna. V současné době nejsou vyloučeny útoky na dispečerské systémy, které ovládají různá technická zařízeni. Řeč je o rozvodných sítích vody, plynu, elektřiny a taky dopravních sítích, při napadení kontroly leteckého provozu, vlakových signálů nebo sítích komunikačních.

Tím, co už bylo řečeno, lze konstatovat, že v mnoha případech zasažení jedné ze zmiňovaných sítí může mít velmi negativní dopady ekonomické, politické a také psychický dopad na obyvatelstvo. Kromě toho se jednotlivé dopady mohou prolínat mezi sebou.

2.3 Kybernetické útoky a jejich výskyt

Následující kapitola se věnuje způsobům pomoci, kterých je možno již zmíněné metody kybernetického terorismu praktikovat.

Nejdřív, než se do toho pustím, vysvětlím, co je kybernetickým útokem. Obecně kybernetický útok (Cyber Attack) je možné definovat jako cílenou kybernetickou aktivitu zaměřenou proti celé řade zdrojů působících v rámci kybernetického

[27] *Co je počítačový virus + druhy virů: Adware* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/adware/
[28] *Co je počítačový virus + druhy virů: Spyware* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/spyware/

prostoru, zejména narušení důvěrnosti, integrity nebo dostupnosti informací.[29] Každý kybernetický útok má svá specifika a vzhledem k tomu existuje sedm fází kybernetického útoku:

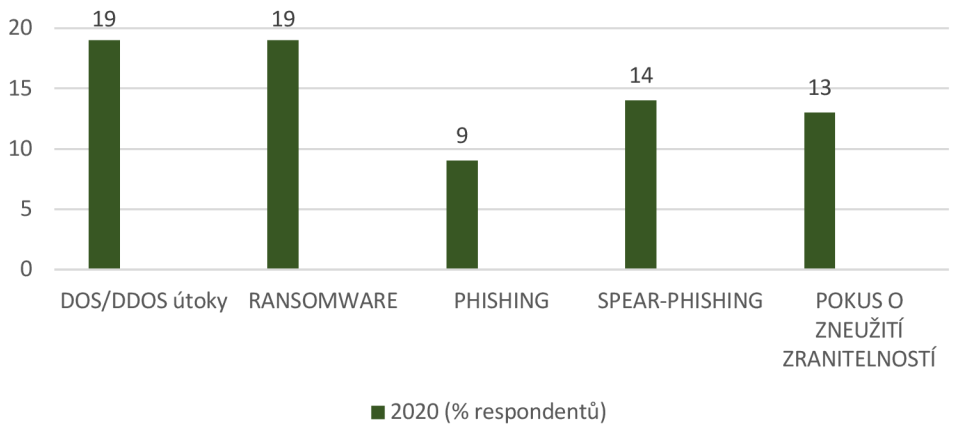
- průzkum neboli výběr cílů
- vyzbrojení (spárování malwaru)
- doručení pomocí sociálního inženýrství
- zneužití
- instalace
- Command and Control
- ilegální činnost k dosažení operačních cílů.[30]

Celý proces je perfektně technicky zpracovaný a finančně náročný.

Rozlišujeme mezi několika druhy kybernetických incidentů, ale ve své práci se následně budu věnovat pouze těm nejčastějším kybernetickým útokům, se kterými se setkáme v rámci kyberterorismu.

Na úvod k tomu chci uvést graf, kde budou zařazené nejzávažnější typy kybernetických útoků za rok 2020. Data byla získána na základě vyhodnocení dotazníků v rámci hodnoceni stavu kybernetické bezpečnosti v ČR Národním úřadem pro kybernetickou a informační bezpečnost.[31]

[29] Jak probíhá kybernetický útok?: Kybernetická bezpečnost. *Axians.CZ* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/
[30] KRAUS, Josef. *Kyberválka:* definice, historie. Masarykova univerzita. Brno, 2016.
[31] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020: kybernetická bezpečnost v roce 2020 pohledem českých institucí, organizací a firem 1* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf



Graf 2 Nejzávažnější typy kybernetických útoků v roce 2020 – sestavila autorka

Z grafu je patrné, že převažují DoS/DDoS útoky a ransomware, které se následně pokusím popsat a vysvětlit jejich podstatu.

DoS (Daniel of Service) útoky – jedná se o nejčastěji používané a zároveň i doposud nejnebezpečnější útoky. Jejich podstatou je tzv. odepření služby, znamená to, že mají za cíl omezit nebo narušit přístup k počítačovému systému nebo síti. Obvykle se zaměřují na servery, aby znepřístupnily webové stránky a platební služby. Brání uživatelům v přístupu k online informacím nebo službám, které potřebují, zejména jsou to: emailové schránky, internetové bankovnictví, online zpracováni plateb apod.[32] Pochopitelně DoS útoky mohou byr realizované v různých formách a mít zaměření na různé služby. Z tohoto hlediska rozlišujeme tři typy DoS útoku:

- DoS směrované na fyzické zničení či změny síťových komponentů,
- DoS se zaměřením na zničení či změny informací o konfiguraci,
- DoS cílem kterých je spotřeba vzácných, omezených či neobnovitelných zdrojů.[33]

[32] *CERT.NZ*: *Denial-of-service.* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.cert.govt.nz/individuals/common-threats/denial-of-service/
[33] *CERT.NZ: Preparing for denial-of-service incidents.* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.cert.govt.nz/it-specialists/guides/preparing-for-denial-of-service-incidents/

Důležitým kritériem pro realizaci takto zaměřených incidentů je potřeba mít odpovídající prostředky, zejména technické vybavení a připojeni k síti Internet.

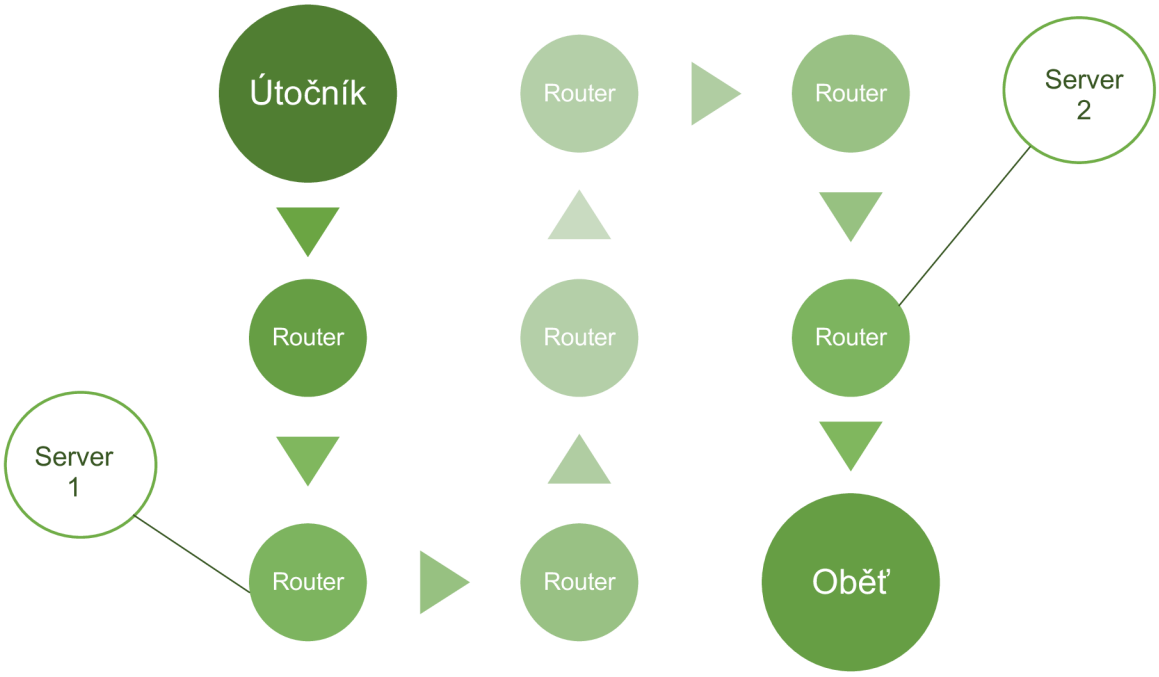


Schéma 2 Proces běžného DoS útoku – sestavila autorka

Na přikladu daného schématu běžného Dos útoku se dá popsat, jak takový typ útoku probíhá. Nejprve si útočník vyhlédne oběť, respektive počítač, na který bude utočit. K tomu zpracovává seznam zařízení, v daném případě routeru, pomocí kterých bude uskutečňovat napadeni na určitý cil. Následně musí navázat spojení s počítačem oběti prostřednictvím exploitu[34], který k útoku použije a dalším krokem je už zahájeni samotného útoku. Program zvolený útočníkem pracuje s IP adresou routeru ze seznamu, falšuje zdrojovou adresu a nastavuje ji na IP adresu oběti.[35]

Vice rozvinutou variantou DoS útoků a jejich podmnožinou jsou DDoS (Distributed Daniel of Service) prováděné způsobem, pomocí kterého útočník se snaží zahltit linku oběti prostřednictvím velkého množství jiných počítačů. Zajímavé je, že útočník tyto počítače nepotřebuje přímo napadnout a pouze je využívá k dosažení

[34] Exploit v informatice je speciální program.
[35] HALLER, Martin. *Denial of Service útoky: reflektivní a zesilující typy: Jak takový útok probíhá?* [online]. 2006 [cit. 25.11. 2021]. Dostupné z: https://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/

svého cíle. Najednou mohou útočit stovky nebo tisíce počítačů. Základním kritériem těchto druhů útoku je, že jsou distribuované. Princip zůstává stejný jako u DoS útoku zobrazeném na schématu č. 2 „Proces běžného DoS útoku“, ale je propracovanější a má vetší počet vazeb.[36]

Vedle DoS útoku k nejzávažnějším patří i Ransomware. Pod Ransomware rozumíme specifický druh škodlivého kódu, který se používá většinou k vydíraní. Podstatou je uzavřeni přístupů k počítací nebo šifrovaní jeho obsahu. Následně útočník vyžaduje u vlastníka finanční prostředky k zpřístupnění zařízení a odblokovaní dat.[37]

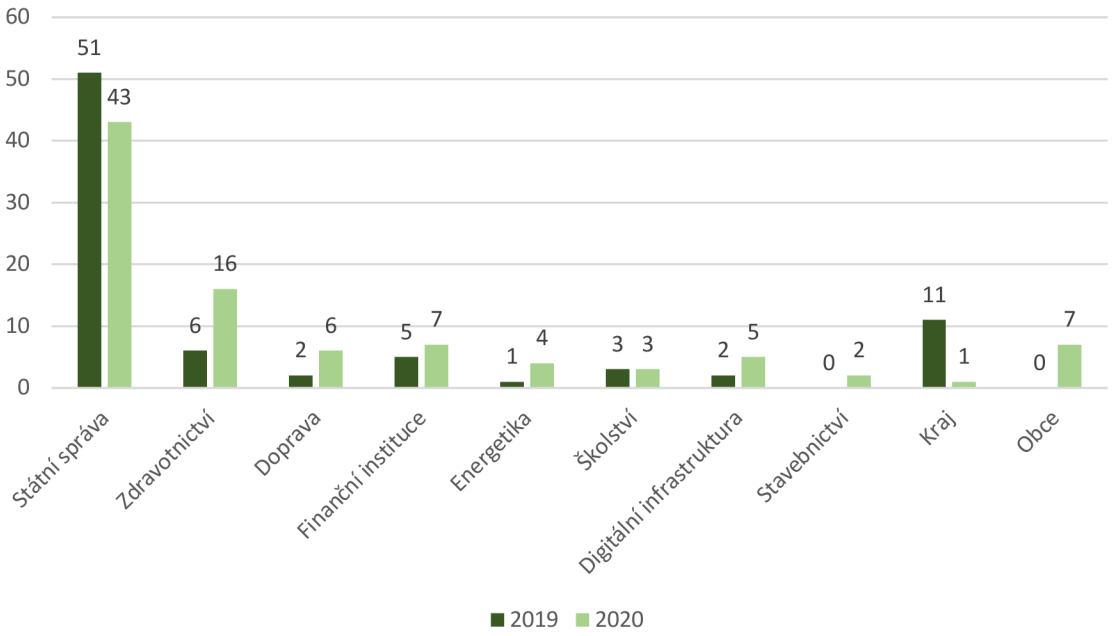
Také v rámci této problematiky se chci zmínit o *Hackingu* jako neautorizovaném přístupu k počítačovému systému nebo síti pomocí níž se dá určitou mírou poškodit daný systém. Tady hacker může po získaní přístupu k systému přenést informace a data na další systém, neboli místo krádeže informací může pozměnit jejich obsah.

Existuje velké množství potenciálních cílů, na které se dá útočit a jejichž napadení by mělo nepříznivé následky pro dotyčné osoby. Příkladem objektů kybernetického útoku mohou být:

- statni orgány, obchodní korporace, a to za účelem vydíraní
- operační a informační střediska (OPIS) integrovaného záchranného systému (IZS), která koordinuji tyto složky a používají společný systém pro koordinaci
- dodavatelé energie a ostatních služeb za účelem vyřazení z provozu a další.[38]

[36] Tamtéž.
[37] Ransomware: Co je ransomware?. *Eset Progress. Protected* [online]. [cit. 01. 12. 2021]. Dostupné z: https://www.eset.com/cz/ransomware/
[38] Audit národní bezpečnosti: *Kyberterorismus* [online]. Praha, 2016 [cit. 01. 12. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

To nám ukazují i statistické údaje NÚKIB, kde v roce 2020 byl zaznamenán desetinásobný nárůst kybernetických incidentů oproti roku 2019, za kterým stoji vyšší počet kybernetických útoku.[39]



Graf 3 Vývoj počtu kybernetických incidentů v letech 2019 a 2020 dle odvětví [40] – sestavila autorka

Z grafu vyplývá, že nejvíce zasaženými oblastmi jsou státní správa a sektor zdravotnictví, jako klasické cíle útoku v kyberprostoru. Na základě analýzy kybernetických incidentů NÚKIB uvádí, že za třetinou řešených událostí stály škodlivé kódy, které tvořily ransomware. Další část případu vyústila v omezení dostupnosti služeb, systémů nebo webových portálů v důsledku DDoS útoků.[41]

[39] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020: kybernetická bezpečnost v roce 2020 pohledem českých institucí, organizací a firem 1* [online]. [cit. 01. 12. 2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf
[40] Tamtéž.
[41] Tamtéž.

2.4 Charakteristika kybernetických útočníků

V pozadí každého kybernetického útoku stoji cracker[42], který tyto útoky programuje a ty jsou následně vedeny kybernetickými prostředky. Snaží se naháčkovat do systému či sítě dle vlastního prospěchu, nebo k dosaženi určitého cíle. Aby došlo ke kybernetickému incidentu, respektive útoku, musí pachatel mít odpovídající úroveň znalostí a dovedností.

Proto rozlišujeme čtyři kategorie subjektu v mezích kyberprostoru:

- pachatelé internetové kriminality
- hacktivisty
- kyberteroristy
- kybernetické válečníky.[43]

Ve své diplomové práci nebudu popisovat pachatele internetové kriminality, jelikož to není vyloženě moje téma, ale zbývající tři subjekty se pokusím co nejpřesněji charakterizovat.

Hacktivisté obecně nazývaní hackři, kteří využívají svých znalostí a dovedností pro politické nebo sociálně motivované účely. Jsou to skupiny jedinců, kteří se sjednocují k provedeni jednotlivých kybernetických útoků. V odborné literatuře pod pojmem hacktivismus se rozumí: *„Politický motivovaná jednotlivá online akce nebo kampaň vedená nestátními aktéry s cílem vyjádřit nesouhlas nebo upozornit na problém obhajovaný hacktivisty“.*[44]

---

[42] Cracker je termín pro programátora s obstojnými znalostmi programování, který se snaží vědomě zneužit sít či systémy.
[43] BALDI, Stefano, Eduardo GELBSTEIN a Jovan KURBALIJA. *Hacktivism, Cyber-Terrorism and Cyberwar: The activities of the uncivil society in cyberspace* [online]. Switzerland: DiploFoundation, 2003. [cit. 03. 12. 2021]. ISBN 99932-53-01-4. Dostupné z: https://books.google.cz/books?id=oKS2RtaKDm8C&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
[44] SAMUEL, Alexandra Whitney. *Hacktivism and the Future of Political Participation: Introduction: Into the world of hacktivism* [online]. Cambridge, 2004. [cit. 03. 12. 2021]. Dostupné z: https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

Co se týče motivace hacktivistu, tak ta je primárně závislá na tom, jak jednotlivec nebo skupina jednotlivců vnímá určité procesy, které se odehrávají ve společnosti. Je téměř výhradně nějakým způsobem politicky nebo i nábožensky orientovaná a zaměřená na ovlivňovaní názorů ostatních na konkrétní problém. V tu chvíli, když se hacktivistům podaří naverbovat další osoby a upoutat pozornost médií, tak začínají hledat tzv. slabá místa, která lze v rámci cílových organizací zneužít. V následku toho je pak prováděn kybernetický útok. Útoky hacktivisty mohou zahrnovat znehodnocení webových stránek, hromadné rozesílání e-mailů, útoky DoS nebo DDos a mnoho dalších metod. Příčiny útoků mohou být různé, ale primárně zahrnují taková témata, jako jsou občanská práva, náboženství, demokracie atd. V současné době je každá významná změna ve společností podporovaná nebo napadená různými aktivistickými skupinami, demonstranty a má prvek hacktivistické podpory, i když to není zjevné.

Jestliže běžné kybernetické útoky mohou páchat specialisté různé úrovně znalostí a dovedností, tak kyberteroristé a kybernetičtí válečníci se považuji za profesionály nejvyššího úrovně, pomineme-li morální a etickou stránku jejich činnosti. Při těchto zločinných aktivitách nemusí jednat pouze jedna osoba, ale mohou to být i teroristické skupiny zaměřené na útoky v kyberprostoru, jinak řečeno, jako heckerský gang. Kyberteroristé a kybernetičtí válečníci mohou mít politické, ideologické nebo náboženské důvody pro páchaní kybernetických útoků, které mohou být podporovány jak politickým systémem, tak dokonce i státem, zejména se jedná o finanční podporu. V tomto případě kybernetičtí válečníci používají jak na národní, tak i mezinárodní úrovni tzv. kybernetickou zbraň k získání cenných dat a dosahování vojenských a politických cílů.

V závěru teto kapitoly se dá říci, že jsou to odborníci s vysokou úrovní kvalifikace, schopni proniknout a poškodit bezpečnost počítačových systémů s následujícími vlastnostmi:

- před kybernetickým útokem jsou maximálně vyzbrojeni znalostmi o systému, na který budou útočit, jeho softwaru a jeho administrátorů
- kontrolují programy a cvičí s metodami hackování na vytvořeném modelu se stejnými ochrannými prvky jako na zaměřeném cíli

- snaží se nabourat do bezpečnostního systému počítače co nejrychleji, aby nebylo možné hned si všimnout útoku a přijmout odpovídající opatřeni
- jednají pod falešným jménem a skrývají svojí IP adresu v síti
- často používají softwarové záložky, které se mohou samy zničit v případě, když budou objeveny.[45]

3. Koncept kybernetické bezpečnosti

V předchozí kapitole jsem se pokusila předložit základní oblasti činnosti, ke kterým teroristé využívají kyberprostor. Z toho nám vyplývá, že se internet využívá velmi různorodým způsobem. Vzhledem k technologickému rozvoji ze schématu č. 1 „Chronologie nejznámějších typu virů“ je také vidět, že teroristé se dokážou rychle přizpůsobovat nově vznikajícím možnostem, které se jim v této oblasti nabízejí. Bezpečnost online prostoru se stále více přenáší do reálného světa a má přímý vliv na bezpečnost státu a jeho obyvatel. Proto i příslušné orgány musí reagovat na nové potenciální hrozby, které souvisí s pronikáním terorismu do kyberprostoru.

Pro pochopení významu kybernetické bezpečnosti je potřeba nejdřív definovat tento pojem. Existuji různé definice, ale ve své práci jsem uvedla jen ty, které považuji za nejvíc charakterizující.

Pod pojmem kybernetická bezpečnost (Cybersecurity) rozumíme: *„Soubor technologií, postupů a praxe k ochraně počítačů, počítačových sítí a dat před neoprávněným přístupem, zranitelností a útoky spáchanými kybernetickými zločinci“.*[46] Všeobecně se dá říct, že jde o ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována celková bezpečnost informací na prostorech internetu.

Další významnou definicí je podle Policejní akademie ČR v Praze ta, kterou vydala spolu s Českou pobočkou AFCEA ve Výkladovém slovníku kybernetické

[45] *Кто такие хакеры?: Так кто же такие «хакеры»? SPY-SOFT.NET* [online]. [cit. 03. 12. 2021]. Dostupné z: https://spy-soft.net/pro-xakerov-kto-takie-xakery/
[46] MRÁZEK, Josef. Mezinárodní právo v kybernetickém prostoru: 1. *k pojmům kybernetické bezpečnosti a kybernetických útoků* [online]. 2014. [cit. 05. 12. 2021]. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2014/7/2.Mrazek_7_2014.pdf

bezpečností, kde se uvádí tento pojem jako: „Souhrn právních, organizačních, technických a vzdělávacích prostředků směrujících k zajištěni ochrany kybernetického prostoru“.[47]

Také je důležité zmínit další definici, podle které je kybernetická bezpečnost: *„Souborem nástrojů, zásad, bezpečnostních konceptů, bezpečnostních opatření, pokynů, přístupů k řízení, rizik, akcí, školení, osvědčených postupů, záruk a technologií, které lze použít k ochraně kybernetického prostředí, organizace a aktivit uživatelů“.*[48]

Z výše popsaných definic je patrné, že společným aspektem a charakteristickým znakem kybernetické bezpečnosti je ochrana před krádeží a zneužitím důležité informace. Koncept kybernetické bezpečnosti je relativně nový, neboť v posledních letech se vše aktivně digitalizuje a spolu s tím přibývá vice citlivých informací uložených v počítačích, které jsou napojené na internet.

3.1 Systém zajišťování kybernetické bezpečnosti v ČR

Kyberprostor není omezen hranicemi, nabízí teroristům anonymitu a ztrátu stop jejich zločinných jednání. Prevence, vyšetřovaní a trestání pachatelů je velmi obtížným procesem. Hovoříme-li o prostředcích boje proti kyberterorismu, můžeme definovat tři základní oblasti, které se ovšem vzájemně prolínají a ovlivňují:

[47] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 3 aktualizované vyd. [online]. Praha: Policejní akademie ČR v Praze, 2015. [cit. 05. 12. 2021]. ISBN 978-807-2514-366. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

[48] *ITU Committed to connecting the world: Definition of cybersecurity* [online]. [cit. 05. 12. 2021]. Dostupné z: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

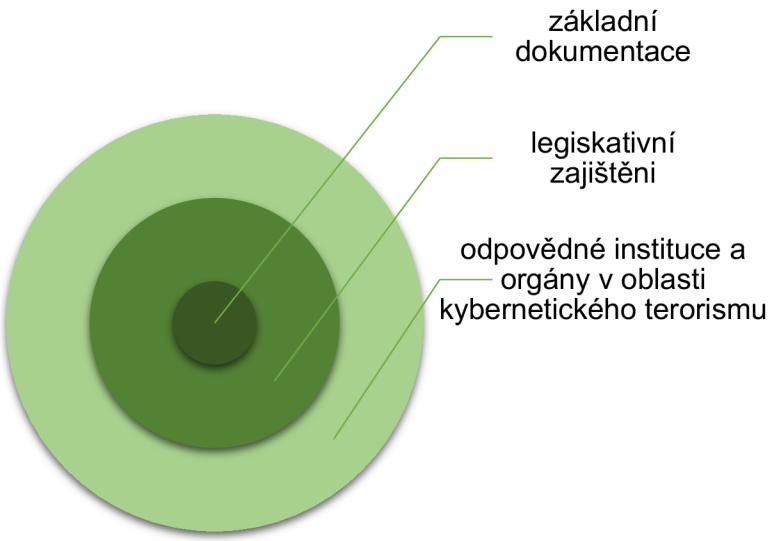


Schéma 3 Základní oblasti boje proti terorismu – sestavila autorka

V dalších podkapitolách se budu věnovat každé oblasti zvlášť.

3.2 Základní dokumentace v oblasti kybernetické bezpečnosti

Základním, strategickým a koncepčním dokumentem pro zajišťovaní bezpečnosti České republiky je Bezpečnostní strategie ČR z roku 2015, kam patři i problematika kybernetické bezpečností. Na tento dokument navazuje Národní strategie kybernetické bezpečností ČR jako stěžejní dokument upravující strategický rámec zajištující online bezpečnost. Její aktualizace je podmíněna závaznou dobou pěti let, přičemž specifické časové naplnění bude vycházet z konkrétních úkolů stanovených v Akčním plánu kybernetické bezpečnosti ČR na období let 2021-2025. Sem také patří Strategie rozvoje ICT služeb veřejné správy a její opatření na zkvalitňovaní dané činnosti.

3.3 Legislativní zajištění bezpečnosti kyberprostoru v ČR

V České republice oblast kybernetické bezpečnosti upravuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB). Tento právní předpis je první českou úpravou v dané problematice. Zákon ukládá povinnost všem příslušným organům k zajišťovaní bezpečnosti a také upravuje působnost NÚKIB jako orgánu, který má na starosti koordinace a dozor nad zajišťováním

kybernetické bezpečnosti ČR. V roce 2017 proběhla novela zákona o kybernetické bezpečnosti, a to zákonem č. 205/2017 Sb., s účinností od 1. srpna prostřednictvím zákona č. 104/2017 Sb., s účinností od. 1. července.

Provádějícími právními předpisy k tomuto zákonu jsou vyhlášky a nařízeni vlády. Mezi ně patří – vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidací dat. Následně bylo v tomto směru aktualizováno nařízení vlády č. 432/2010. Sb., o kritériích pro určení prvku kritické infrastruktury.

Kybernetické trestné činy jsou upraveny zákonem č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. Zejména jsou to tyto TČ:

- § 230 Neoprávněný přistup k počítačovému systému a nosiči informací,
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti,
- § 257a Poškození a zneužití záznamu na nosiči informací.

Dále tam lze zařadit i následující paragrafy:

- § 290 Získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou,
- § 311 Teroristický útok,
- § 312 Teror.

3.4 Odpovědné instituce a orgány v oblasti kyberterorismu

Systém zajišťovaní kybernetické bezpečnosti v ČR je potřeba brát komplexně. Nejdřív se zmíním o tom, že přístup České republiky k udržení bezpečného digitálního prostředí byl od samého počátku založen na aktivní a efektivní spolupráci

všech subjektů jak na národní, tak i mezinárodní úrovni, kde každý aktér má jasně stanovené povinnosti a pravomoci.[49]

Za zajišťovaní bezpečnosti na území našeho státu je odpovědna vláda ČR, která je vrcholným orgánem výkonné moci. K její hlavním úkolům patři řízení a funkčnost celého bezpečnostního systému ČR.

Gestorem dané problematiky a zároveň ústředním správním orgánem pro oblast kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který vznikl na základě zákona o kybernetické bezpečnosti a převzal kompetence od Národního bezpečnostního úřadu (NBU). Má odpovědnost za veřejně regulované služby v rámci družicového systému Galileo.[50] Součástí NÚKIB je Národní centrum kybernetické bezpečnosti (NCKB) jakož jeho výkonná sekce, která zejména zajišťuje prevenci před kybernetickými hrozbami, koordinace spolupráce na národní i mezinárodní úrovni při řešení incidentů a probíhajících útoků.[51]

V rámci NCKB je provozován vládní CERT (GovCERT.CZ), který má klíčovou roli při ochraně kritické informační infrastruktury a dalších důležitých informačních a komunikačních systémů a sítí. Institut CERT zavedl zákon o kybernetické bezpečnosti, ten byl upraven v § 20 tohoto zákona, tam jsou vymezeny i jeho kompetence. Od roku 2011 také působí i národní CERT, je upraven v § 17 zákona o kybernetické bezpečnosti. Ten je provozován sdružením CZ.NIC. Je to soukromá osoba a její funkce a role vyplývají z veřejnoprávní smlouvy uzavřené mezi ní a NÚKIB.[52] Národní CERT byl zřízen na základě směrnicí Evropského

---

[49] ŘEHKA, Karel. Národní strategie kybernetické bezpečnosti České republiky: Úvodní slovo. *NÚKIB* [online]. [cit. 09. 12. 2021]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[50] NÚKIB: O NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 09. 12. 2021]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[51] NÚKIB: NCKB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 09. 12. 2021]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

[52] *Národní strategie kybernetické bezpečnosti České republiky: System zajišťování kybernetické bezpečnosti ČR* [online]. [cit. 09. 12. 2021]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů na území EU.

Hlavním gestorem elektronizace výkonu veřejné správy (eGovermentu) je Ministerstvo vnitra (MV), které je také zodpovědným orgánem za provoz řady informačních a komunikačních systémů, které jsou důležité pro řádné fungovaní státního aparátu. Vztahy a spolupráce s ostatními státy a mezinárodními organizacemi koordinuje Ministerstvo zahraničních věcí (MZV) v oblasti kybernetické bezpečnosti ve spolupráci s NÚKIB a dalšími dotčenými orgány.

Zpravodajské služby České republiky se také podílí na zajišťovaní bezpečnosti v kyberprostoru. Působnost a činnost těchto služeb vymezuje zákon

č.153/1994 Sb., o zpravodajských službách České republiky. Především poskytují zpravodajské informace příslušným organům státní správy, zpracovávají je a provádějí následně analýzy.

Dalším důležitým aktérem bezpečnostního systému je Policie ČR jako největší bezpečnostní sbor. V boji s hrozbami v kyberprostoru je národním kontaktním bodem a zodpovědným pracovištěm PČR v rámci této problematiky Národní centrála proti organizovanému zločinu, Služby kriminální policie a vyšetřování (NCOZ SKPV). Taky PČR náleží potírání a prevence závadových aktivit v síti Internet, konkrétně orgánům činným v trestním řízení.

Neméně důležitým orgánem v systému zajišťování kybernetické bezpečnosti je resort Ministerstva obrany, který se zabývá kybernetickou obranou státu proti nežádoucím zásahům do komunikačních a informačních systémů a vojenských sítí. Na kybernetické obraně se podílejí jak Vojenské zpravodajství, tak i Armáda ČR, zejména Velitelství kybernetických sil a informačních operací (VeKySIO). Tyto orgány úzce spolupracují a jejich schopnosti se vzájemně prolínají.

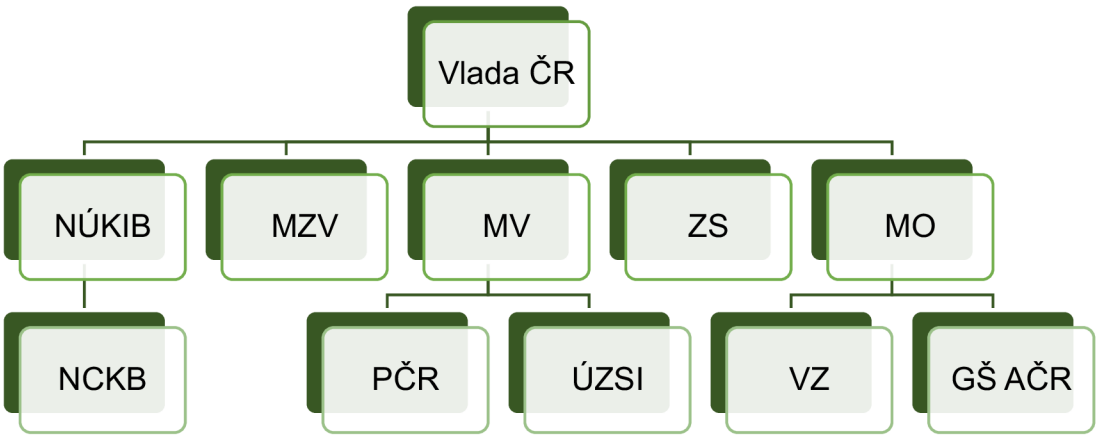


Schéma 4 Struktura zajišťovaní kybernetické bezpečnosti České republiky – sestavila autorka

Dané schéma stručně ukazuje strukturu orgánů, které zajištují bezpečnost v kyberprostoru. Jak jsem již uváděla výše, je ta problematika komplexní a dost rozšiřující se, proto lze říct, že tento systém netvoři pouze mnou uvedené subjekty, ale i další instituce, které jsou klíčové ve svých oblastech působností a prostřednictvím jejichž práce lze předcházet různým kybernetickým incidentům. Zejména jsou to orgány a osoby uvedené v § 3 zákona o kybernetické bezpečnosti.

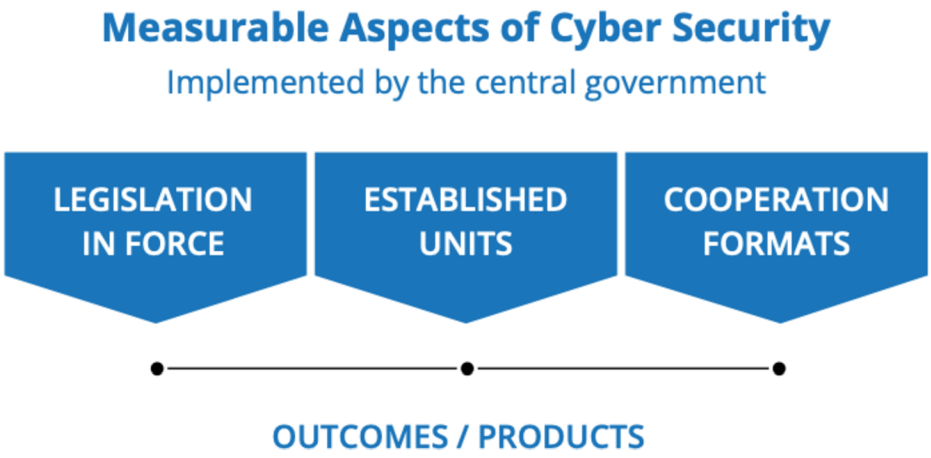
3.5 Úroveň kybernetické bezpečností České republiky

Úroveň kybernetické bezpečnosti České republiky lze zjistit na základě estonské analýzy e-Gavernance Academy (eGA) podle indexu národní kybernetické bezpečnosti (national cyber security index, NCSI). Index NCSI je globálním nástrojem měření připravenosti států na kybernetické hrozby a útoky. Spolu s tím se jedná o globální databázi národních dokumentů v oblastí kyberbezpečnosti.

Česká republika patři podle indexu NCSI mezi TOP 10, kde zaujímá čtvrté místo mezi 160 států světa. Naše země je hodnocena jako jedna z nejlépe připravených v rámci prevence kybernetických hrozeb a jejích odhaleni. Index NCSI zahrnuje čtyři důležité aspekty:

- platná legislativa,

- orgány a instituce (existence výkonných organizací),
- vnitrostátní spolupráce,
- výsledek činností (cvičení, doporučení).[53]



Obr. 2 Kategorie kybernetické bezpečnosti [54]

Vetší pozornost je věnovaná právním předpisům, výkonným subjektům a jejích spolupráci. V těchto kategoriích mohou země získat vetší počet bodů.

3.6 Opatření k řešení výzev a hrozeb v oblasti kybernetické bezpečnosti

Jelikož současný svět je plně digitalizován a čelí jak mnou výše popsaným hrozbám, tak i ostatním, musí existovat i nějaké řešení k těmto rychle se měnicím podmínkám. V rámci kybernetické bezpečnosti řeč je o kybernetických opatřeních, která ve své podstatě zajišťuji vetší důvěru občanů v digitální nástroje a služby. Česká republika v zájmu bezpečnosti svých občanů aktivně pracuje nad legislativním rámcem a přispívá k tvorbě unijních právních norem s ohledem na aktuální výzvy a vznikající jednání státních a nestátních aktérů v kyberprostoru.[55]

[53] *National Cyber Security Index 2018: Methodology* [online]. Tallinn: e-Governance Academy Rotermanni 8, 10111 Tallinn ega.ee, 2018 [cit. 13. 12. 2021]. Dostupné z: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf
[54] Tamtéž.
[55] *Národní strategie kybernetické bezpečnosti České republiky: Mezinárodní právní rámec* [online]. [cit. 13. 12. 2021]. Dostupné z:

Vzhledem k tomu, že teď prožíváme náročnou dobu a celý svět bojuje s pandemií COVID-19, tak je podle mě důležité zmínit se o opatřeních NÚKIB v oblastí zdravotnictví, kde vzhledem k situaci s novou nemocí je vyšší tlak na poskytování lékařských služeb a počet meziročních kybernetických incidentů v sektoru zdravotnictví v roce 2020, který vzrostl o 267 % oproti roku 2019. Rok 2020 přinesl s sebou nový trend cílených ransomwarových útoků na různé typy nemocníc a zejména v ČR došlo k zašifrovaní sítí Fakultní nemocnice v Brno a Psychiatrické nemocnice Kosmonosy. Na tyto události hned reagoval NÚKIB a podle zákona o kybernetické bezpečností vydal reaktivní opatření k minimalizací rizika incidentu. Taky NÚKIB v rámci vlastních možností nabídl dalším subjektům, které mohou být dotčeny podobným incidentem, konzultace a podporu při provedení specifické činností.

Mezí další ne méně důležité oblastí řadíme sektor veřejné správy a infrastrukturu, které Česko v průběhu ostatních několika let usilovně digitalizuje. V těchto sférách ČR podporuje využívání unifikovaných kanálů, prostřednictvím kterých probíhá bezpečná výměna informací a dat.

Mezi efektivní způsoby opatřeni lze zanést také spolupráci mezi orgány, které se zabývají kybernetickou bezpečností. ČR se snaží udržovat kvalifikované pracovníky a vytváří pro ně patřičné pracovní podmínky. Taky se stále hledají nové talenty, pro které se vytváří vhodné pracovní prostředí a tímto motivuje lidi pracovat pro státní organizace nebo bezpečnostní složky. Takže pro případ závažného ohroženi ČR lze využít i kybernetických expertů pracujících vně státní správy, zejména expertů z akademického, soukromého nebo i neziskového sektoru.[56]

Významným nástrojem, který přispívá v oblasti kybernetické bezpečností je kvalitní vzdělávaní a edukativní projekty, které cílí na osvojení potřebných návyků pro bezpečný pohyb v kyberprostoru. V roce 2019 nastal výrazný vzestup poptávky po cvičeních v rámci této problematiky a podíleli se na tom vedoucí pracovních zúčastněných institucí. V témže roce proběhla velice přínosná cvičení pro orgány

---

https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[56] Tamtéž.

činné v trestním řízení, státní správu a energetický sektor. Kromě zodpovědných orgánů státní správy ČR se zaměřila i na všechny věkové skupiny uživatelů digitálních technologií, především dětí a seniorů, které jsou nejrizikovější kategorií. Mezi celorepublikové vzdělávací aktivity v oblasti kybernetické bezpečnosti patří například Internetem bezpečně, E-Bezpečí a Chytrá škola. Projekty, kterými se zabýval NÚKIB, se staly Městečko kybernetov, Digitální stopa, Senzační senioři i Network Security Monitoring Cluster.[57]

4. Fenomén kybernetické války

Internet a jeho rozvoj je ukázkovým příkladem, jak mohou technologie zjednodušit život člověka, ale existuje i velice negativní stránka technologického pokroku. Některé negativní aspekty už byly popsány výše a teď se chci zmínit o takovém fenoménu jako je kybernetická válka.

V dnešní době se internet jako virtuální prostor považuje za prostředí, kde se mohou odehrávat vojenské konflikty, vedle země, vody, vzduchu a vesmíru, to bylo označeno na summitu NATO od roku 2016. Počet bezpečnostních kybernetických incidentů včetně kyberútoku v posledním desetiletí výrazně stoupl a spolu s tím se začalo diskutovat o tzv. kybernetické válce, která se už dostala do vojenských doktrín řady zemí. Česká republika není výjimkou a aktivně pracuje nad obranou proti kybernetickým hrozbám.

4.1 Vymezení pojmu kybernetická válka

Specialisté na dané téma mají dost odlišné názory na tento specifický problém, například velitel informačních a kybernetických sil, brigádní generál Miroslav Feix, M.S. je dost opatrný u pojmů kybernetická válka a zejména u slova „válka“. Říkal, že pro něho to znamená: „jeden státní aktér a tisíc mrtvých za rok“.[58] Považuje to

[57] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019: Opatření* [online]. [cit. 27. 12. 2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf?fbclid=IwAR1_iSzWOCnPaEX3simzsNffxPUcEVtAP4wtJA4CfsOnT9OBaii4AeDVMUQ

[58] FEIX, Miroslav. *Kybernetická válka zatím neprobíhá, útoky hackerů jsou spíš zastrašování* [online]. 2019. [cit. 27. 12. 2021]. Dostupné z: https://www.youtube.com/watch?v=hrtzPnmqNig&t=25s

prostě za „faktický stav, kde se odehrávají informační operace“.[59] Ve své podstatě je tomu tak. Jinými slovy, když politická reprezentace nějakého státu rozhodne pro demonstrace a použití síly, vyšle vojáky na konkrétní misi, tak oni mohou používat různé dezinformace, působit prostřednictvím informací na nepřítele, následně jeho poškodit. Pozoruhodným příkladem je aktuální válečný konflikt mezi Ruskem a Ukrajinou, kde ruské zpravodajské služby GRU a ruští hackeři podnikají kyberútoky schopné zablokovat ukrajinské operátory mobilní sítě, televizní vysílaní, vyřadit z provozu webové služby apod., stejně jak to bylo při anexi Krymu.

Ale abychom porozuměli vymezení kybernetické války, tak je zapotřebí nejdříve definovat tento pojem. Zde uvedu definice, které považuji za nejpřesnější z těch, které se mi podařilo najit a se kterými lze souhlasit.

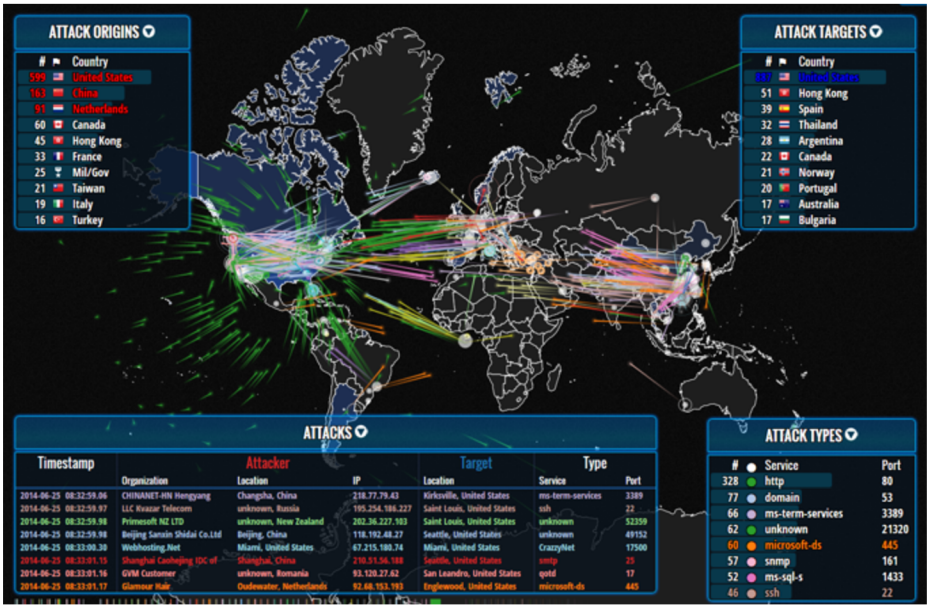
Ve vztahu ke kyberterorismu je kyberválka: „*Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem, je tzv. kyberprostor“.* [60] Podle definice uvedené v slovníku kybernetické bezpečnosti, je kybernetická válka: *„Použitím počítačových technologií k vedení války v kybernetickém prostoru. Oproti jiným druhům kybernetických incidentů se odlišuje v tom, že se vztahuje konkrétně na politicky motivované útoky, na vládu, stát a jiné organizace vládního charakteru“.*[61] Převážné jsou to aktivity spojené se získáním citlivých informací nebo vyřazení z provozu technologické infrastruktury země, na kterou je zaměřen útok.

Podstatou kybernetické války je pak samotný boj mezi znepřátelenými stranami, který se odehrává v mezích kyberprostoru, a je to bohužel dnešní realitou. Kybernetický boj ve své podstatě není odlišný od konvenčního boje a platí tam podobná pravidla podle mezinárodního humanitárního práva. Přesněji se jedná o *„Soubor právních norem mezinárodního práva veřejného, které upravují vedení*

---

[59] Tamtéž.
[60] RAŠEK, Antonín. Kybernetická válka pokračuje. Vojenské rozhledy. [online]. 2013, č. 4 [cit. 03. 01. 2022]. ISSN 1210-3292. Dostupné z: https://vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/kyberneticka-valka-pokracuje
[61] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Kybernetická válka*. 3 aktualizované vyd. [online]. Praha: Policejní akademie ČR v Praze, 2015. [cit. 03. 01. 2022]. ISBN 978-807-2514-366. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

ozbrojených konfliktů s cílem zmírnit utrpení a omezit materiální škody či jiné negativní dopady, které tyto konflikty způsobují".[62] Jak to vypadá v kyberprostoru, vidíme na následujícímu obrázku.



Obr. 3 Kybernetická válka v reálnem čase [63]

Pro lepší pochopeni procesu vedení kybernetické války uvedu čtyři hlavní oblasti, které jsou postižené při vedení kybernetického konfliktu mezi nepřátelskými zeměmi:

- vládní servery (stránky prezidenta, parlamentu, ministerstev)
- bankovní systémy (fungovaní ekonomiky států)
- informační a komunikační systémy (zablokování 4G a 5G)
- energetická soustava zemí.

[62] JUKL, Marek. *Zdravotnický instruktor Českého červeného kříže.* 2 uprav. vyd. [online]. Praha: Úřad Českého červeného kříže, 2006. [cit. 03. 01. 2022]. ISBN 802544547X. Dostupné z: https://www.cervenykriz.eu/files/files/cz/mhp/cojemhp.htm

[63] *Why the U.S. Shouldn't Play Games With Cyberwarfare as Its Power Declines* [online]. [cit. 03. 01. 2022]. Dostupné z: https://www.pressenza.com/2021/04/why-the-u-s-shouldnt-play-games-with-cyberwarfare-as-its-power-declines/

V tu chvíli, když tyto oblasti jsou deaktivovány v napadené zemi už je vyvolán chaos a panika mezi obyvatelstvem. Dochází ke zhoršení politické, ekonomické a sociální situace.[64]

4.2 Prostředky kybernetického boje

Každý boj musí být vedený pomocí určitých nástrojů a v našem případě kybernetických nástrojů. Proto v kontextu kybernetické války je třeba definovat kybernetické zbraně. Kybernetické zbraně jsou velmi mocné, zejména z hlediska páchaní komplexní trestné činnosti z jednoho místa po celém světe a velkou mírou anonymity, tudíž složitého vyhledávaní útočníků. Obecně pod tím pojmem rozumíme škodlivý software, malware atd. používaný na národní nebo mezinárodní úrovni pomocí kterého dochází k získávání cenných dat a dosahování vojenských a politických cílů, například Stuxnet. Mají obrovský efekt a negativně ovlivňují naše každodenní činnosti, aniž bychom si všimli, že se děje něco zvláštního, třeba pomalejší internet.

Významná definice kybernetické zbraně je uvedena v Talinském manuálu 2.0, který zpracovalo 19 právníků pro vlády států na případ kybernetických konfliktu, podle něho *„jsou to kybernetické způsoby bojů, které jsou používány, navrženy a plánované pro způsobení následků, které lze identifikovat jako způsobené kybernetickým útokem“.*[65] V současnosti nejznámější subjekty, které používají kybernetickou zbraň jsou: USA, Čína a Rusko, dalšími jsou: Francie a Izrael a Velka Británie.

Pochopitelně kybernetickou válku neomezuji ani vzdálenost, ani fyzické hranice státu, fakticky hrozí všem. Není zde klasická reakční doba, jaká je v konvenčních válkách, je finančně nenáročná a stala se součástí klasických vojenských operací. Kupříkladu, když vidíme vojenskou techniku, tanky apod., tak se budeme bránit obdobným způsobem a víme čeho se očekávat, ale kybernetický útok přichází

---

[64] BÍLÝ, Miloš. *Ohrožuje nás kybernetická válka?* [online]. [cit. 03. 01. 2022]. Dostupné z: https://rehabilitovani-vojaci.cz/files/ohrozuje-nas-kyberneticka-valka.pdf

[65] *Tallinn Manual 2.0 on the international law applicable to cyber operations* [online]. Cambridge University Press, 2017. [cit. 13. 01. 2022]. Dostupné z: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

nečekaně. Jediná obrana je neustálé monitorovaní bezpečnostní situace v kybernetické doméně. Podrobněji rozeberu problematiku obrany proti hrozbám vyplývajícím z kyberprostoru v následující časti práce.

4.3 Obrana proti kybernetickým hrozbám

V rámci kybernetických konfliktů hraje klíčovou roli kybernetická bezpečnost a kybernetická obrana. Ve své práci se budu zabývat kybernetickou obranou se zaměřením na resort obrany České republiky.

Podle zákona č. 222/1999 Sb., o zajišťovaní bezpečností ČR obrana je definovaná takto: *„Souhrn opatřeni k zajištěni svrchovanosti, uzemni celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému“.*[66] Kybernetická obrana je potom brána jako součást obranného plánovaní ČR ve smyslu zákona o zajišťovaní obrany a věnuje se jí dnes velká pozornost.

Logické je, abychom se mohli něčemu bránit, zapotřebí včas identifikovat a následně eliminovat hrozby. V dnešní době podle Auditu národní bezpečností existuje celkem pět konkrétních hrozeb v kyberprostoru, které mohou ohrozit ČR a její národní bezpečnost:

- kybernetická špionáž
- narušení nebo snížení odolnosti IT infrastruktury
- nepřátelské kampaně
- narušení nebo snížení bezpečnosti eGovernmentu
- kyberterorismus.[67]

Vzhledem k tomu, že s postupem času se navyšuje počet ofenzívních a defenzivních kybernetických operací potenciálně nepřátelských státu, Česká republika

[66] Zákon č. 222/1999 Sb., o zajišťovaní bezpečností České republiky v posledním znění
[67] *Audit národní bezpečnosti: Hrozby v kyberprostoru* [online]. Praha, 2016 [cit. 17. 01. 2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

odráží hrozby kybernetického charakteru v Národní strategií kybernetické bezpečností pro období let 2015-2020, kde stanoví úkoly pro posilování schopností kybernetické obrany a vedení operací v souladu s požadavky NATO ve Cyber defence z roku 2019.

Vedle strategie existuje Akční plán pro dosaženi cílů, podle kterého je Vojenské zpravodajství pověřeno zajišťovat kybernetickou obranu našeho státu. Také na základě tohoto dokumentu Vláda ČR zadala VZ vybudovat centrum, které bude schopno pracovat a provádět operace v kyberprostoru. Tím pádem vzniklo i Národní centrum kybernetických operací (NCKO), které pomáhá vojenskému zpravodajství jak v zahraničních operacích AČR v rámci NATO nebo EU, tak i v případě výskytu kybernetického konfliktu za účelem obrany ČR.[68]

Dalším významným dokumentem přímo zaměřeným na dané téma je Strategie kybernetické obrany pro období 2018-2022, rozdělená na veřejnou a neveřejnou část. Stanovuje koncepční podmínky pro řádné zajišťovaní obrany státu v kyberprostoru a uvádí, že *„připravenost na kybernetické útoky musí být komplexní a nemůže se zaměřit pouze na sféru bezpečností, nutné budovat schopnosti i proti útokům, které lze vyhodnotit jako způsobilé aktivovat obranu státu“.*[69] Z toho vyplývá, že ČR pracuje nad všemi možnými variantami hrozeb a kybernetická obrana je připravena čelit těm nejzávažnějším útokům. Mezí základní strategické cíle Strategie kybernetické obrany 2018-2022 prostřednictvím kterých by mělo být dosaženo náplně strategie patří:

- Nastavení právního rámce
- Vybudování a rozvoj infrastruktury NCKO
- Vybudování schopností obrany v kyberprostoru
- Nastavení spolupráce a provádění vzdělávání a cvičení

[68] RIETHOFOVÁ, Alžběta. *Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR* [online]. [cit. 17. 01. 2022]. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/

[69] *Strategie kybernetické obrany ČR 2018-2022* [online]. Národní centrum kybernetických operací. [cit. 17. 01. 2022]. Dostupné z: https://www.vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf

- Podílení se na zajištění kybernetické bezpečnosti v resortu MO.[70]

Dle mého názoru každý z těchto cílů je velmi důležitý pro dosažení jediného globálního cíle, za který se 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“.[71]

Uvažuji, že v tomto ohledu je třeba věnovat zvláštní pozornost metodám, které vedou k dosažení těchto cílů a základní strategické směřování brát komplexně. Nelze opomenout jednu z těch funkcí, systém zajišťovaní kybernetické obrany musí pracovat v integraci a tím i zabezpečovat stabilní bezpečnostní situaci. Taky je potřeba neustále vyhodnocovat na jaké úrovni je náplň strategie a co jí ještě chybí.

[70] Tamtéž.
[71] Tamtéž.

Praktická část

5. Řízený strukturovaný rozhovor s odborníky na dané téma

5.1 Metodologie výzkumů

Praktická část práce navazuje na teoretickou a seznamuje s výsledky vlastního zjišťování úrovně kybernetických incidentů v rámci kyberprostoru, které hrozí poškozením počítačových sítí či zařízení se závažnými dopady na bezpečnost státu a také na civilní obyvatelstvo České republiky.

Vedle kyberterorismu v této části diplomové práce uvedu i mnou zjištěné dílčí aspekty kybernetické bezpečnosti České republiky, zejména legislativní zajištěni bezpečnosti v kyberprostoru.

Pro získáni relevantních dat jsem využila formu řízeného strukturovaného rozhovoru na daná témata. Problematika kyberterorismu a kybernetické bezpečností je následně podrobněji zpracovaná pomocí expertní metody strategické analýzy SWOT.

5.2 Cíle

Nedostatek zkušeností ve světové i domácí praxi s problematikou kyberterorismu, rozvoje účinných společenských a právních mechanismů boje proti kyberterorismu tedy vyžaduje koncepční pochopení tohoto tématu a kvalitního opodstatnění. Hledají se cíle, rysy a trendy, způsoby, jak minimalizovat hrozby v kyberprostoru a umět rozlišovat kybernetickou kriminalitu a útoky kyberterorismu. To jsou důvody, které vedly k volbě oslovit odborníky zabývající se touto problematikou, a to formou strukturovaného rozhovoru.

Cílem strukturovaného rozhovoru bylo získaní informací o aktuálním stavu kyberterorismu v České republice, jeho nejzávažnějších útocích a nejvíce napadených subjektech, zejména v současné době, když prožíváme celosvětovou pandemií COVID-19. Taky cílem bylo získat informace o stavu kybernetické bezpečnosti České republiky a případných opatřeních v rámci této problematiky.

Na základě výsledků, které byly zjištěny formou strukturovaného rozhovoru, je zpracována SWOT analýza, která poukazuje na připravenost České republiky čelit kybernetickým útokům a z nich plynoucím hrozbám.

5.3 Otázky pro rozhovor a jejích stručná charakteristika

V této části diplomové práce se já jako autorka věnuji otázkám, které byly součástí strukturovaného rozhovoru s oslovenými subjekty. Uvádím základní informace ke každé otázce, z čehož je patrné, na co přesně je zaměřena diskuse. Za tímto účelem jsem zvolila následující otevřené otázky:

1. Čím se zabýváte?

- informace o životu a praxi respondenta

2. Jaká je Vaše praxe (zkušenosti) s kyberterorismem?

- otázka je zaměřená na získaní poznatků o praktické činnosti osloveného účastníka rozhovoru

3. Co osobně vnímáte pod pojmem kyberterorismus?

- možnost odborníka vyjádřit svůj názor k problematice

4. Jaký je rozdíl mezi kybernetickou kriminalitou a kyberterorismem?

- vzhledem k tomu, že kybernetické incidenty konané pomocí stejných prostředků, je důležité rozlišovat, který útok je v rámci kyberkriminality a který je považován za akt kyberterorismu, otázka umožnuje vyjádřit respondentovi názor na chápaní těchto pojmů

5. Jaké metody, prostředky používají kyberteroristé na prostorách internetu?

- možnost se vyjádřit o trendech, cílech a způsobech současného kyberterorismu, pokud respondent měl s tím praxi

6. Jak hodnotíte Českou právní úpravu kybernetické bezpečnosti?

- tato otázka umožnuje oslovenému vyjádřit svůj subjektivní názor na právní rámec České republiky v souvislosti se zajišťováním kybernetické bezpečnosti

7. Jak vidíte koncept bezpečnosti z pohledu plnění kritérií zákona o kybernetické bezpečnosti?

- tato otázka je zaměřena na získáni informací, jak respondent vnímá a hodnotí zajišťováni bezpečnosti v mezích kyberprostoru

8. Jaká jsou pravidla kybernetické války a jak jsou mocné kybernetické zbraně?

- otázka umožňuje oslovenému účastníkovi vyjádřit se k problematice kybernetického boje

9. Myslíte si, že hrozí Česku kybernetická válka a jak se ji bránit?

- subjektivní názor respondenta, na danou kybernetickou hrozbu

10. Doplnění informací, které považujete za podstatné.

- možnost se zmínit o tom, co tady nezaznělo ale podle názoru respondenta je důležitou připomínkou.

V příloze dané práce přiřadím odpovědi každého z respondentů a v následujících částech sepíšu celkové hodnoceni každého rozhovoru na dané téma.

5.4 Vyhodnoceni rozhovoru s pracovníkem Oddělení informačních systémů a komunikačních technologií, Útvaru policejního vzdělaní a služební přípravy Policie České republiky

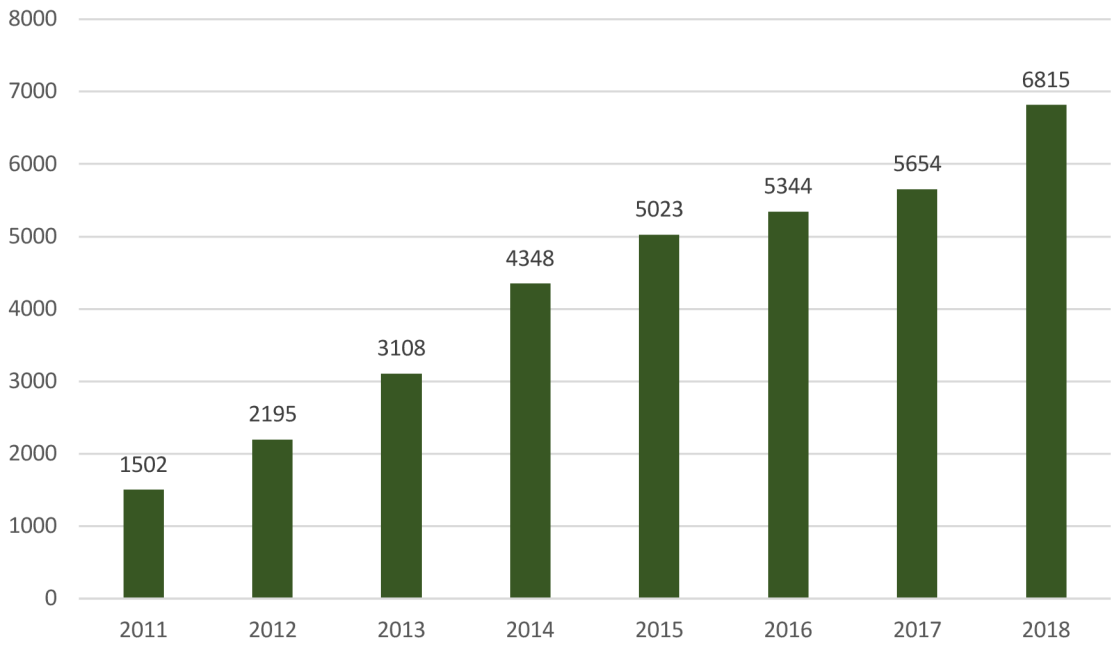
Ke strukturovanému rozhovoru o kyberterorismu a kybernetické bezpečnosti jsem se rozhodla oslovit pplk. Mgr. Martina Koláře, který pracuje na odd. informačních

systémů a komunikačních technologií, útvaru policejního vzdělaní a služební přípravy PČR. Jeho praxe u PŠR je osmnáctiletá, z toho se osm let věnuje TČ v rámci kyberkriminality na základě útvaru a taky se zabývá různými druhy kybernetických incidentů v kyberprostoru. Podle něj je současný rozvoj informačních systémů a komunikačních technologií velmi rychlý a počet uživatelů internetu stále se navyšuje. Ze statistik vychází, že při porovnání s 28 zeměmi Evropské unie pozice České republiky za rok 2018 v počtu k internetu připojených domácností byla pod unijním průměrem a pohybovala se v rozmezí přibližně 30 %.

Vzhledem ke zvýšené aktivitě v kyberprostoru se objevila nová společensky škodlivá jednání, a to od běžné kybernetické kriminality po závažné útoky kyberterorismu. O kyberterorismu budeme hovořit i v případě, že cílem nebo nástrojem teroristů je informační nebo komunikační systém. Moderní informační a komunikační technologie hrají důležitou roli při šíření hrozby terorismu. Z pohledu trestněprávní ochrany se jedná o nejmladší obor, který se rychle rozviji, přizpůsobuje aktuálním podmínkám a je odvětvím kriminálního prostředí. Ve své podstatě jde o trestnou činnost, která je páchaná v prostředí informačních a komunikačních technologií včetně počítačových sítí.

Samotná oblast ICT je buď předmětem útoku, nebo jde o nedovolená jednání páchána za využití ICT, jakož v dnešní době významného prostředku k páchaní trestné činností. Ze své praxe pplk. Mgr. Martin Kolář uvádí, že předmětem kybernetických útoků jsou většinou informace a veškerá osobní data, která jsou uložena na datových úložištích, nebo která chce pachatel podvodným způsobem vylákat. Podle respondenta je cílem vládní systém, politika, doprava, ekonomické procesy a také zdravotnictví. Z mnoha výzkumů vyplývá, že za poslední dva roky se navýšil počet kybernetických útoků na zdravotní sektor a finanční průmysl, to vše díky světové pandemií COVID-19. Také e-mailové phishingové útoky byly nejčastějším zdrojem narušení dat při práci z domova. V dubnu 2020 roku Google blokoval denně 18 milionů malwaru a phishingových e-mailů souvisejících s koronavirem.

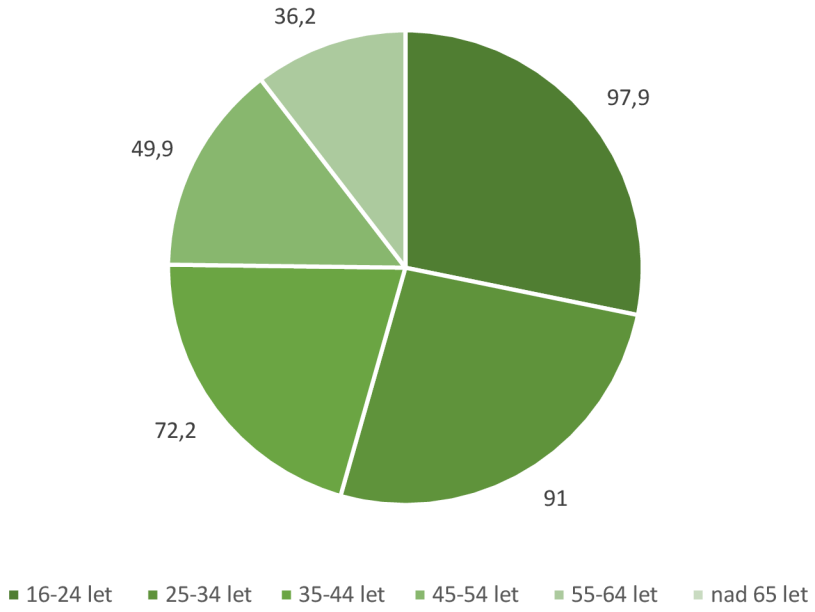
Policie ČR sleduje počet kybernetických incidentů už od roku 2011 a pokaždé se ukazuje vzrůstající trend.



Graf 4 Nárůst trestné činnosti kybernetických incidentů 2011-2018 – sestavila autorka

V roce 2018 bylo na internetu evidováno 6815 kybernetických incidentů, což ve srovnání s rokem 2017 potvrzuje nárůst o více než 1000 skutků. Podle statistik NÚKIB v roce 2020 už bylo zaznamenáno 8073 případů kriminality páchané na internetu. Velmi významných kybernetických incidentů řešených NÚKIB bylo celkem 9.

Problému, kterému bychom měli dle pplk. Mgr. Martina Koláře věnovat pozornost je pak povědomí lidí o internetové bezpečnosti a celkové chování lidí na internetu, zejména otevírání neznámých příloh, pochybných internetových stránek apod. V Česku pro soukromé účely využívají internet kolem 80 % osob – tedy naprostá většina uživatelů – a pro pracovní účely (alespoň 1x týdně) kolem 9,2 %.



Graf 5 Procento osob podle demografie, které využívají denně služeb internetu – sestavila autorka

Data zahrnuji procento osob, které internet využívají aktivně, jinak mezi celkovou populací osob starších 65 let při zahrnuti všech by šlo pouze o 7,9 procent.

Dle pplk. Mgr. Martina Koláře kybernetická bezpečnost je relativně nový obor, kterému třeba věnovat zvláštní pozornost, a to z důvodu, že musí přicházet se stále novými a efektivními řešeními, jelikož cílem Evropské komise je zabezpečit globální internet pomocí efektivních bezpečnostních nástrojů.

V dané problematice se neustále hledají účinné prostředky pro boj s kyberterorismem. Metody kyberterorismu a vedle toho i kybernetické zbraně jsou velmi účinné z hlediska možnosti páchání komplexní trestné činnosti z jednoho místa po celém světě. Charakterizují se velkou mírou anonymity, tudíž složitého vyhledávání pachatelů.

V případě vypuknuti kybernetické války, tak ta podle názoru respondenta hrozí všem státům, ČR není výjimkou. Také pplk. Mgr. Martin Kolář je každopádně toho názoru, že ve skutečností neexistuji žádná pravidla boje, která by měla být jako

v opravdové válce a jediná obrana je neustálá aktivní obrana a bezpečné chování uživatelů na internetu.

5.5 Vyhodnoceni rozhovoru s odborníkem v oblastí ochrany utajovaných informací (OUI)

Dle mého názoru oblast ochrany utajovaných informaci souvisí s tématem kyberterorismu, jelikož ve většině případů útoky ovlivňují politickou scénu, kde hackerovi jde o cenné informace a data, která mohou být pozměněna, vymazána nebo ukradena z jiných důvodu. Internet díky své povaze představuje pro teroristy užitečný nástroj pro získávání informací. Tím pádem může dojit k poškozeni řídicího aparátu a systému s celkem velmi nežádoucími následky. Proto jsem oslovila odborníka pro oblast OUI Karla Šimana, pracovníka resortu MV ČR, který ve svém oboru má 30 letou praxi.

Dle názoru p. Šimana je zřejmě, že problematika utajovaných informací a jejich ochrana je vyňata ze zákona o kybernetické bezpečnosti, jelikož OUI upravuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ale na tomto místě je velmi důležitá spolupráce mezi subjekty. Vyřazeni nebo zneužiti informací podle tohoto zákona může způsobit újmu zájmu ČR nebo může být pro tento zájem nevýhodné, stejně jako i podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Podle § 21 ods. 1 zákona o KB může být vyhlášen stav kybernetického nebezpečí. Pod tímto pojmem se rozumí 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 pádem by mohlo dojit k porušení nebo případně ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. Z toho vyplývá, že provázanost prvky a spolupráce těchto dvou oborů je dokonce zakotvena v právních předpisech ČR.

Vzhledem k tomu, že zákon o kybernetické bezpečnosti se inspiroval zahraničními vzory p. Šiman považuje ho za kvalitní a dostačující stejně jako i prováděcí vyhlášky a nařízení k tomuto zákonu.

Co se týče problému kybernetické války, neboli jak ještě tomu říkají informační války v kyberprostoru, tak respondent se drží názoru, že válka nemá pravidla, cílem je vyhrát za každou cenu. Také podle Šimana nelze jednoznačně definovat účinnost kybernetických zbraní, a to z důvodu, že tam působí příliš mnoho faktorů. Účinnou obranou v případě kybernetického napadení by měla být možnost selektivního odpojeni síťových infrastruktur, šifrování síťového provozu a dodržovaní bezpečnostních opatření požadovaných zákonem o kybernetické bezpečnosti.

Na závěr k vyhodnocení tohoto rozhovoru chci se zmínit o tom, že Karel Šiman se ještě doposud nesetkal v oblasti OUI s žádným bezpečnostním incidentem v souvislosti s kyberterorismem, ale neznamená to, že k tomu nemůže dojit v blízké budoucnosti.

6. Výsledky, které byly zjištěny řízeným strukturovaným rozhovorem

Hlavním cílem praktické časti diplomové práce bylo prozkoumat problematiku kyberterorismu a spolu s ním i účinných opatřeni v bojí proti útokům odehrávajícím se v mezích kyberprostoru. Za tímto účelem jsem oslovila dva respondenty blízké k dané problematice, kteří mně vyšli vstříc s možností realizace řízeného strukturovaného rozhovoru. Na základě vyhodnoceni jejich odpovědí v této kapitole se budu věnovat SWOT analýze stavu kyberterorismu a kybernetické bezpečnosti v České republice, kam jsem zařadila výsledky vyplývající z rozhovorů.

6.1 SWOT analýza

V rámci rozhovorů s respondenty na vybrané téma byly zjištěny následující informace:

Silné stránky

- Legislativní zajištěni kybernetické bezpečnosti jak vnitrostátní, tak i mezinárodní zpracované na velmi vysoké úrovni.

- Udržování zahraničních vztahů v souvislosti s danou problematikou, především se světovou komunitou CERT/CSIRT týmů a mezinárodními organizacemi.
- Spolupráce v oblasti kybernetické bezpečnosti mezi subjekty veřejného, akademického a soukromého sektoru v rámci České republiky.
- Rychlá reakce na řešení kybernetických bezpečnostních incidentů.
- Efektivní osvětová a školící činnost vybraných cílových skupin.

Slabé stránky

- Nedostatek kvalifikované pracovní síly v oblasti kybernetické bezpečnosti.
- Nízká úroveň povědomí obyvatelstva České republiky o kybernetické bezpečnosti.
- Nedostatek finančních prostředků vynaložených na danou problematiku.
- Těžko odhalitelní pachatelé kybernetických útoků.
- Nedostatek preventivních opatření v souvislosti s kybernetickými útoky.
- Neexistence hranic v rámci kyberprostoru.

Příležitosti

- Provádění analýzy trendů v oblasti kyberterorismu a kybernetické bezpečnosti.
- Každoroční účast na různém druhu tréninků a kybernetických cvičení na národní a mezinárodní úrovni.
- Neustálá práce nad národními bezpečnostními standardy a aktualizace právní úpravy v oblasti kybernetické bezpečnosti.
- Včasné vyhodnocení rizik v oblasti kyberterorismu a přijímání příslušných opatření.
- Snaha o vytvořeni pracovního prostředí, které motivuje specialisty v daném oboru pracovat pro státní organizace.
- Zapojení kybernetických expertů vně státní správy.
- Snaha o provádění pravidelné kontroly dodržování požadavků zákona o kybernetické bezpečnosti.

- Kvalitní zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech.
- Příprava bezpečnostních standardů pro informační systémy a komunikační technologie.

Hrozby

- Narušení sociální integrity.
- Poškození cenných informací a dat.
- Neautorizovaný přístup k datům včetně prozrazení utajovaných skutečností.
- Působení cizích států v kyberprostoru na území České republiky.
- Nárůst množství kybernetických útoků v mezích kyberprostoru.
- Zneužívání kyberprostoru teroristy pro účely získání vlastního prospěchu nebo výhody.
- Propaganda a podněcování nespokojenosti u společnosti v mezích kyberprostoru.

Význam mé praktické časti práce spočívá v tom, že mnou zjištěné výsledky vyplývající z řízených rozhovorů s respondenty, mohly by být použity pro lepši pochopení daného téma a současného stavu kyberterorismu na našem území. Také by se mohly stát přínosem budoucího rozvoje problematiky kyberterorismu a kybernetické bezpečnosti.

Cenné rady pro zavadění preventivní činnosti a zdokonalovaní už existujících opatření by se daly využit pro plánováni budoucích aktivit v rámci kyberprostoru. Ze SWOT analýzy vyplývá, jakým oblastem bychom měly věnovat pozornost orgány podílející se na zajišťovaní kybernetické bezpečnosti České republiky.

Závěr

V závěru mé diplomové práce se chci zmínit o hlavním problému kybernetické problematiky a zejména relativně novém typy terorismu, který vznikl v rámci kyberprostoru. Hlavním cílem bylo důkladně prozkoumat dané téma a dokázat, že nebezpečí pro společnost nejen trvá, ale ve spojitosti s bezpečnostní situací ve světě i narůstá. Žádný ze států včetně České republiky si nemůže byt jistý, že má dost prostředků a způsobů pro eliminací hrozeb vyplývajících s kybernetických útoků.

Podle mého názoru boj proti počítačovým útokům, včetně těch, které představují hrozbu kyberterorismu, by měl být zaměřen k zabezpečení kyberprostoru a minimalizací dopadu kyberterorismu na vládní systémy a civilní obyvatelstvo. Rozumným řešením se zdá zabezpečení na úrovni poskytovatele s výkonnými systémy filtrování obsahu, detekce a blokování škodlivých kódů a jakýchkoli podobných aktivit.

Při důkladném prozkoumaní kybernetické problematiky jsem zjistila, že tento jev se dokáže velmi rychle se přizpůsobit změnám probíhajícím v kyberprostoru. Zvýšení hrozby terorismu v souvislosti s rozvojem informačních a telekomunikačních technologií vedlo od konce 70. a počátku 80. let 20. století k trvalému vědeckému zájmu o příčinách tohoto jevu, jeho podstatě o analýze organizačních forem a činností teroristických organizací. Orgány zajištující kybernetickou bezpečnost by měly usilovat o včasné identifikace kyberteroristických hrozeb, o účinnou politiku boje proti nim a minimalizaci následků kybernetických útoků. Progresivní potlačení a předčasná identifikace kybernetických útoků je ale bohužel otázkou budoucnosti.

Tempo informačního rozvoje, které je zodpovědné za transformaci ekonomických, sociálně-politických a kulturních procesů v moderní společnosti, vyžaduje účinné mechanismy státní regulace informačních systémů a komunikačních technologií.

Témata, která byla zvolena v této práci, nám přiblížila danou problematiku a upozornila na aspekty, kterým by se měla věnovat maximální pozornost specialistů. Doufám, že prostřednictvím zvoleného postupu jsem splnila zadané téma.

Seznam literatury

Monografie:

1. BRZYBOHATÝ, Marian. *Terorismus I.* Praha: Police History, 1999. ISBN 80-902670-1-7.
2. MAREŠ, Miroslav. *Terorismus v ČR.* 1. vyd. Brno: Centrum strategických studií, 2005. ISBN 80-903333-8-9.
3. VEGRICHTOVÁ, Barbora. *Hrozba radikalizace: terorismus, varovné signály a ochrana společnosti.* Praha: Grada, 2019. ISBN 978-802-7120-314.
4. BRZYBOHATÝ, Marian, et al. *Terorismus a my: Základy sebeobrany.* 1. vyd. Praha: Computer Press, 2001. ISBN 80-7226-584-9.
5. KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.
6. BALDI, Stefano, Eduardo GELBSTEIN a Jovan KURBALIJA. *Hacktivism, Cyber-Terrorism and Cyberwar: The activities of the uncivil society in cyberspace* [online]. Switzerland: DiploFoundation, 2003. [cit. 03. 12. 2021]. ISBN 99932-53-01-4. Dostupné z: http://books.google.cz/books?id=oKS2RtaKDm8C&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
7. MRÁZEK, Josef. Mezinárodní právo v kybernetickém prostoru: 1. k pojmům kybernetické bezpečnosti a kybernetických útoků [online]. 2014. [cit. 05. 12. 2021] Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issue/2014/7/2.Mrazek_7_2014.pdf
8. JUKL, Marek. *Zdravotnický instruktor Českého červeného kříže.* 2 uprav. vyd. [online]. Praha: Úřad Českého červeného kříže, 2006. [cit. 03. 01. 2022]. ISBN 802544547X. Dostupné z: https://www.cervenykriz.eu/files/files/cz/mhp/cojemhp.htm
9. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Kybernetická válka*. 3 aktualizované vyd. [online]. Praha: Policejní akademie ČR v Praze, 2015. [cit. 03. 01. 2022].

ISBN 978-807-2514-366. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

Časopisecké články:

1. Terorismus a měkké çíle: Definice terorismu. *Ministerstvo vnitra České republiky* [online]. [cit. 25.10. 2021]. Dostupné z: https://www.mvcr.cz/cthh/clanek/definice-terorismu.aspx
2. Terorismus: Typologie terorismu. *Ministerstvo vnitra České republiky* [online]. [cit. 01.11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d
3. Terorismus: Klasické teroristické metody. *Ministerstvo vnitra České republiky* [online]. [cit. 01. 11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d
4. Terorismus: Moderní teroristické metody. *Ministerstvo vnitra České republiky* [online]. [cit. 01. 11. 2021]. Dostupné z: https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09MQ%3d%3d
5. JANOUŠEK, Michal. *Kyberterorismus: terorismus informační společnosti* [online]. [cit. 01.11. 2021]. Dostupné z: https://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html
6. Audit národní bezpečnosti: Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR. Hrozby v kyberprostoru. *Ministerstvo vnitra České republiky* [online]. Praha, 2016. [cit. 15. 11. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
7. COLLIN, Barry. Future of Cyberterrorism: The physical and virtual worlds converge. *Crime and Justice International Volume: 13 Issue: 2* [online]. 1997. [cit. 15. 11. 2021]. Dostupné z: https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge

8. Audit národní bezpečnosti: Třídění hrozeb. *Ministerstvo vnitra České republiky* [online]. Praha, 2016. [cit. 15. 11. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
9. DENNING, Dorothy E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* [online]. 1999. [cit. 15. 11. 2021]. Dostupné z: https://nautilus.org/global-problem-solving/activism-hacktivism-and cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/
10. GORDON, Sarah. *Cyberterrorism* [online]. Symantec Security Response. 2003 [cit. 15. 11. 2021]. Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.7114&rep=rep1&type=pdf
11. *Terrorist Designations and State Sponsors of Terrorism: Foreign Terrorist Organizations* [online]. U.S. Department of state [cit. 15. 11. 2021]. Dostupné z: https://www.state.gov/foreign-terrorist-organizations/
12. *Al-Fateh – The Hamas Web Magazine for Children: Indoctrination to Jihad, Annihilation and Self-Destruction* [online]. Institute for Monitoring Peace and Cultural Tolerance in School Education, 2009. [cit. 15. 11. 2021]. Dostupné z: https://www.impact-se.org/wp-content/uploads/2016/04/Al-Fateh_Report_2009_final.pdf
13. HEICKERÖ, Roland. *Terrorism online and the change of modus operandi* [online]. Command and Control Research Program (U.S.), 2008. [cit. 15. 11. 2021]. Dostupné z: http://dodccrp.org/events/13th_iccrts_2008/CD/html/papers/209.pdf
14. DRMOLA, Jakub. Konceptualizace kyberterorismu. Vojenské rozhledy. Praha: Ministerstvo obrany České republiky [online]. 2013, č. 2 [cit. 16. 11. 2021]. ISSN 1210-3292. Dostupné z: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/konceptualizace-kyberterorismu
15. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020: Kybernetická bezpečnost v roce 2020 pohledem českých institucí, organizací a firem 1* [online]. [cit. 25. 11. 2021]. Dostupné z:

https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

16. HALLER, Martin. *Denial of Service útoky: reflektivní a zesilující typy: Jak takový útok probíhá?* [online]. 2006 [cit. 25.11. 2021]. Dostupné z: https://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/
17. Audit národní bezpečnosti*: Kyberterorismus* [online]. Praha, 2016 [cit. 01. 12. 2021]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
18. SAMUEL, Alexandra Whitney. *Hacktivism and the Future of Political Participation: Introduction: Into the world of hacktivism* [online]. Cambridge, 2004. [cit. 03. 12. 2021]. Dostupné z: https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf
19. ŘEHKA, Karel. Národní strategie kybernetické bezpečnosti České republiky: Úvodní slovo. *NÚKIB* [online]. [cit. 09. 12. 2021]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
20. *Národní strategie kybernetické bezpečnosti České republiky: System zajišťování kybernetické bezpečnosti ČR* [online]. [cit. 09. 12. 2021]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
21. *Národní strategie kybernetické bezpečnosti České republiky: Mezinárodní právní rámec* [online]. [cit. 13. 12. 2021]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
22. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019: Opatření* [online]. [cit. 27. 12. 2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf?fbclid=IwAR1_iSzWOCnPaEX3simzsNffxPUcEVtAP4wtJA4CfsOnT9OBaii4AeDVMUQ

23. RAŠEK, Antonín. Kybernetická válka pokračuje. Vojenské rozhledy. [online]. 2013, č. 4 [cit. 03. 01. 2022]. ISSN 1210-3292. Dostupné z: https://vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/kyberneticka-valka-pokracuje
24. BÍLÝ, Miloš. *Ohrožuje nás kybernetická válka?* [online]. [cit. 03. 01. 2022]. Dostupné z: https://rehabilitovani-vojaci.cz/files/ohrozuje-nas-kyberneticka-valka.pdf
25. *Tallinn Manual 2.0 on the international law applicable to cyber operations* [online]. Cambridge University Press, 2017. [cit. 13. 01. 2022]. Dostupné z: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf
26. Audit národní bezpečnosti*: Hrozby v kyberprostoru* [online]. Praha, 2016 [cit. 17. 01. 2022]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
27. RIETHOFOVÁ, Alžběta. *Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR* [online]. [cit. 17. 01. 2022]. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/
28. *Strategie kybernetické obrany ČR 2018-2022* [online]. Národní centrum kybernetických operací. [cit. 17. 01. 2022]. Dostupné z: https://www.vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf

Zákonná úprava:

1. Zákon č. 40/2009 Sb., trestní zákoník v posledním znění
2. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v posledním znění
3. Zákon č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění zákona č. 104/2017 Sb., a některé další zákony v posledním znění

4. Zákon č. 222/1999 Sb., o zajišťovaní bezpečností České republiky v posledním znění
5. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění
6. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat v posledním znění
7. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích v posledním znění
8. Směrnicí Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
9. Společný postoj rady, ze dne 27. prosince 2001, o použití zvláštních opatření k boji proti terorismu (2001/931/SZBP)

Webové stránky a elektronické zdroje:

1. Islamic State Hacking Division. DBpedia [online]. [cit. 15. 11. 2021]. Dostupné z: https://dbpedia.org/page/Islamic_State_Hacking_Division#
2. BRZYBOHATÝ, Marian. Cyberterorismus [online]. [cit. 16.11. 2021]. Dostupné z: https://docs.google.com/presentation/d/0B9UHcDuG1unoZ1I3eGU4RDNLcVU/edit?resourcekey=0-vHiXohR0KyqEk_OkgZKFWw#slide=id.p1
3. *Co je počítačový virus + druhy virů: Kdy vznikly viry a jak na ně vyzrát?* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/virus/
4. *Co je počítačový virus + druhy virů: Adware* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/adware/
5. *Co je počítačový virus + druhy virů: Spyware* [online]. [cit. 19. 11. 2021]. Dostupné z: https://www.eset.com/cz/spyware/
6. Jak probíhá kybernetický útok?: Kybernetická bezpečnost. *Axians.CZ* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/

7. *CERT.NZ*: *Denial-of-service.* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.cert.govt.nz/individuals/common-threats/denial-of-service/
8. *CERT.NZ: Preparing for denial-of-service incidents.* [online]. [cit. 25. 11. 2021]. Dostupné z: https://www.cert.govt.nz/it-specialists/guides/preparing-for-denial-of-service-incidents/
9. *ITU Committed to connecting the world: Definition of cybersecurity* [online]. [cit. 05. 12. 2021]. Dostupné z: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
10. NÚKIB: O NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 09. 12. 2021]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
11. NÚKIB: NCKB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 09. 12. 2021]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/
12. *National Cyber Security Index 2018: Methodology* [online]. Tallinn: e-Governance Academy Rotermanni 8, 10111 Tallinn ega.ee, 2018 [cit. 13. 12. 2021]. Dostupné z: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf
13. FEIX, Miroslav. *Kybernetická válka zatím neprobíhá, útoky hackerů jsou spíš zastrašování* [online]. 2019. [cit. 27. 12. 2021]. Dostupné z: https://www.youtube.com/watch?v=hrtzPnmqNig&t=25s
14. *Why the U.S. Shouldn't Play Games With Cyberwarfare as Its Power Declines* [online]. [cit. 03. 01. 2022]. Dostupné z: https://www.pressenza.com/2021/04/why-the-u-s-shouldnt-play-games-with-cyberwarfare-as-its-power-declines/
15. Ransomware: Co je ransomware?. *Eset Progress. Protected* [online]. [cit. 01. 12. 2021]. Dostupné z: https://www.eset.com/cz/ransomware/
16. *Кто такие хакеры?: Так кто же такие «хакеры»? SPYSOFT.NET* [online]. [cit. 03. 12. 2021]. Dostupné z: https://spy-soft.net/pro-xakerov-kto-takie-xakery/

Seznam příloh

1. Přepis řízeného strukturovaného rozhovoru s pracovníkem Oddělení informačních systémů a komunikačních technologií, Útvaru policejního vzdělaní a služební přípravy Policie České republiky pplk. Mgr. Martinem Kolářem.

2. Přepis řízeného strukturovaného rozhovoru s odborníkem v oblastí ochrany utajovaných informací (OUI) Karlem Šimanem.

Příloha 1

Přepis řízeného strukturovaného rozhovoru s pracovníkem Oddělení informačních systémů a komunikačních technologií, Útvaru policejního vzdělaní a služební přípravy Policie České republiky pplk. Mgr. Martinem Kolářem

1. Čím se zabýváte?

V současné době jsem zařazen na odděleni informačních systémů a komunikačních technologií, Útvaru policejního vzdělaní a služební přípravy Policie České republiky. U Policie jsem 18 let a z toho 8 let se zabývám jak klasickými TČ, tak i TČ v rámci kybernetické kriminality na základě útvaru. Potýkal jsem se s delikty v rámci kyberprostoru.

2. Jaká je Vaše praxe (zkušenosti) s kyberterorismem?

Ve své praxi zabývám se spíš kyberkriminalitou a kyberterorismus beru okrajově, sleduji situaci na webových stránkách a sociálních sítích.

3. Co osobně vnímáte pod pojmem kyberterorismus?

Je to aktivita spojená s terorismem v rámci kyberprostoru. Odvíjí se od klasického terorismu a šíří se prostřednictvím internetu. Podporuje určité politické skupiny, ale zejména má komplexní dopad na obyvatelstvo dané země, které je cíleně zastrašováno pomocí různých falešných zpráv.

Celkem využívá sociální sítě v Česku 64 % obyvatel s přístupem k internetu, respektive 51,6 %, pokud bereme i ty, co internet aktivně nevyužívají. Pro soukromé účely sociální sítě využívá 63,3 % osob – tedy naprostá většina uživatelů – a pro pracovní účely (pravidelně, tj. alespoň 1x týdně) pouze 9,2%. Obecně více sociální sítě využívají ženy (67,6 % oproti 60,5 %), 16–24 let vykazuje 97,9 %, 25–34 let 91 %, 72,2 % u demografie 35–44 let, 49,9 procent pro 45–54 let, 36,2 % u 55-64letých, 20,7 % u seniorů nad 65 let. Data jsou pro ty osoby, které internet aktivně využívají. Mezi celkovou populací osob starších 65 let by při zahrnutí úplně všech by šlo pouze o 7,9 procent.

4. Jaký je rozdíl mezi kybernetickou kriminalitou a kyberterorismem?

S kyberkriminalitou jsem začínal v roce 2008. Ta byla označena za trestnou činnost páchanou pomoci informačních systémů a komunikačních technologií. Také byla nazývana tzv. informační kriminalitou. Útočníkovi zde jde víc o finanční zisk nebo uspokojováni svých vlastních potřeb. Kyberterorismus je globálním jevem a útoky jsou zaměřené na celou společnost. V tom je ten hlavní rozdíl.

5. Jaké metody, prostředky používají kyberteroristé na prostorách internetu?

První jsou útoky silou. Zde se útočník snaží zjistit data, poškodit systém, nebo získat jinou výhodu útokem, jehož hlavní stránkou je využití převahy nad obětí. Typickým prvkem je určitá nezávislost prováděného útoku, když není vyžadována přílišná interakce s útočníkem. Útočník spustí program a může jej nechat pracovat samostatně.

Patří sem např.:

- Brute force attack (útok hrubou silou) - jde o způsob útoku, při kterém program zjišťuje veškeré možné kombinace do doby zjištění skutečného hesla.
- Počítačové viry - jedná se o počítačové programy, které tajně pracují v počítači a dále se šíří.
- Převážná část počítačových virů je určena ke škodlivé činnosti (mazání dat, šifrování disku bez možnosti přečtení zašifrovaných dat, obtěžování uživatele, zpomalování systému).
- Worm (červ) - počítačový virus, jehož primárním cílem je šířit se. Využívá chyb systému, nebo uživatelů, napadá systém a následně se jeho prostřednictvím dál šíří. Při optimální situaci je schopen se klonovat tak dlouho, až síť zahltí
- Keylogger (záznam stisknutých kláves) - Speciální software, nebo zařízení, které zaznamenává a případně odesílá informace o stisku kláves.

- Phishing (rybaření) - pachatel se snaží „nahazovat“ návnady a čeká, zda se někdo chytne. Nejčastější forma tohoto útoku probíhá tak, že pachatel rozešle možným obětem emailovou zprávu, kde je například upozorní na to, že byl napaden server společnosti vydávající bankovní karty. Snaží se získávat hesla a piny od bankovních účtů, platebních karet atd.
- Trojští koně - ve většině případů použití trojského koně jde o program ke škodlivé činnosti. Rozdíl mezi trojským koněm a počítačovým virem je, že trojský kůň sám nedokáže vytvářet své kopie.

V roce 2018 bylo na internetu evidováno 6815 trestných činů, což ve srovnání s rokem 2017 potvrzuje nárůst o více než 1000 skutků. V celkovém růstu trestné činnosti v prostředí internetu byly nejčastěji zastoupené různé formy podvodných jednání, nicméně v porovnání s minulými roky byl pozorován vzrůstající trend u trestných činů v oblasti hackingu.

6. Jak hodnotíte Českou právní úpravu kybernetické bezpečnosti?

V současné době ji hodnotím jako dostačující. Trestní zákoník implementuje v uvedených ustanoveních závazky z Úmluvy Rady Evropy o kybernetické kriminalitě a z rámcového rozhodnutí Rady EU 2005/222/SV o útocích proti informačním systémům. Další mezinárodní smlouvy a právní akty EU zavazují ČR k provedení závazků týkajících se veřejně přístupné počítačové sítě.

7. Jak vidíte koncept bezpečnosti z pohledu plnění kritérií zákona o kybernetické bezpečnosti?

Kybernetická bezpečnost je relativně nový obor. Musí přicházet se stále novými a efektivními řešeními. Cílem Evropské komise je zabezpečit globální internet pomocí efektivních bezpečnostních nástrojů, které mají zabránit trestné činnosti ohrožující základní práva všech lidí.

8. Jaká jsou pravidla kybernetické války a jak jsou mocné kybernetické zbraně?

Pravidla by měla být stejná jako v opravdové válce, bohužel se tak neděje. Tallinn Manual 2.0 – 19 právníků sestavilo pravidla pro vlády v případě kybernetických konfliktů. Masivní útoky hackerů donutily vlády se bránit.
Za mne určitě jsou kybernetické zbraně velmi mocné zejména z hlediska možnosti páchání komplexní trestné činnosti z jednoho místa po celém světě a velkou mírou anonymity. Je tam tudíž složité vyhledávání pachatelů. Zbraně- škodlivý software, malware, trojany, atd. mají obrovský efekt, ovlivňují negativně naše životy.

9. Myslíte si, že hrozí Česku kybernetická válka a jak se ji bránit?

Kybernetická válka hrozí všem. Není zde klasická reakční doba, jaká je v konvenčních válkách. Vidíte tanky opevníte se… Kybernetický útok přichází nečekaně. Jediná obrana je neustálá aktivní obrana a bezpečné chování uživatelů na internetu. PREVENCE… což se v Česku neděje. Útoky tzv. hackerů jsou stále častější.

10. Doplnění informací, které považujete za podstatné.

Dnes je dost nízké povědomí lidí o internetové bezpečnosti a celkem rizikové chování lidí na internetu, například (otevírání neznámých příloh, otevírání pochybných internetových stránek, nezajištěný internetový prohlížeč antivirem atd.) Proto potřebujeme řadu efektivních opatření, neustálou efektivní obranu a bezpečný pohyb uživatelů v kyberprostoru.
Při porovnání pozice České republiky za rok 2018 s 28 zeměmi Evropské unie vyplynou dvě podstatné informace: 1. rozdíly v počtu k internetu připojených domácností se mezi jednotlivými státy pohybují v rozmezí přibližně 30% a za 2. ČR je pod unijním průměrem. Nejhůře je na tom Bulharsko, Řecko a Litva, nejlépe Nizozemí, Lucembursko a samozřejmě severské státy. Nad průměrem EU je ještě Velká Británie, Německo, Rakousko, Irsko a silně digitalizované Estonsko.

Příloha 2

Přepis řízeného strukturovaného rozhovoru s odborníkem v oblastí ochrany utajovaných informací (OUI) Karlem Šimanem

1. Čím se zabýváte?

Ochranou utajovaných informací (OUI) podle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve složkách MV ČR.

2. Jaká je Vaše praxe (zkušenosti) s kyberterorismem?

Praxe víc jak 30 let v oblasti viz 1. Vzhledem k nastaveným bezpečnostním opatřením v oblasti OUI jsem se s kyberterorismem nesetkal, žádný bezpečnostní incident neměl v souvislosti s kyberterorismem.

3. Co osobně vnímáte pod pojmem kyberterorismus?

Kyberterorismus jsou politicky motivované činy prováděné prostřednictvím kyberprostoru za účelem způsobení ekonomických škod nebo škod na lidských životech.

4. Jaký je rozdíl mezi kybernetickou kriminalitou a kyberterorismem?

Jde o kriminalitu vykonávanou prostřednictvím kyberprostoru, definovanou jako spektrum aktivit zneužívajících data, počítačové a informační systémy a kyberprostor za účelem osobního, finančního a psychologického zisku. Hlavní rozdíl ve srovnání s kyberterorismem je motivace útočníků.

5. Čím se zabývají kyberteroristé na prostorách internetu?

Viz bod 3. definice kyberterorismu.

6. Jak hodnotíte Českou právní úpravu kybernetické bezpečnosti?

181/2014 Sb., zákon o kybernetické bezpečnosti vzhledem k tomu, že se inspiroval zahraničními vzory je kvalitní a dostačující.

7. Jak vidíte koncept bezpečnosti z pohledu plnění kritérií zákona o kybernetické bezpečnosti?

Zákon o kybernetické bezpečnosti a zejména jeho prováděcí vyhlášky definuje koncept bezpečnosti pro ty, kterých se to týká – subjekty stanovené v § 3 zákona 181/2014.

8. Jaká jsou pravidla kybernetické války a jak jsou mocné kybernetické zbraně?

Válka nemá pravidla, cílem je vyhrát za každou cenu. Účinnost kybernetických zbraní nelze jednoznačně definovat – působí příliš mnoho faktorů.

9. Myslíte si, že hrozí Česku kybernetická válka a jak se ji bránit?

Pokud bude zajištěno dodržování zákona o kybernetické bezpečnosti tak ne, i když hrozba je přítomna vždy. Obrana – možnost selektivního odpojení síťových infrastruktur, šifrování síťového provozu, realizace opatření požadovaných zákonem o kybernetické bezpečnosti.

10. Doplnění informací, které považujete za podstatné.

Nepoužívat termín utajované informace v souvislosti se zákonem o kybernetické bezpečnosti, jejich ochrana je z tohoto zákona vyjmuta.