VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERTERORISMUS A ÚTOKY PROTI INFORMAČNÍM TECHNOLOGIÍM

Autor práce: Jakub Chýlek

Studijní obor: Bezpečnostně právní studia ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2017

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně na základě vlastních zjištění, s použitím odborné literatury a uvedených materiálů.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, trpělivost, připomínky a metodické vedení práce.

ABSTRAKT

CHÝLEK, J. *Kybernetický terorismus a útoky proti informačním technologiím: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2017. 59 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kyberterorismus, kybernetický útok, kyberprostor, informační technologie, hacker

Práce se zabývá problematikou kyberterorismu a kyberprostoru. První část shrnuje informace a pojmy kyberprostoru, terorismu a kyberterorismu. Pojednává blíže o kyberprostoru, jeho definici, dělení a vývoji. Rozebírá dále definice terorismu a porovnává s definicí kyberterorismu. Další část řeší druhy nástrojů a útoků proti informačním technologiím. Dále se zaobírá problematikou hackerů, popisuje jejich vývoj a dělení dle jejich motivace. Navazuje část, která pojednává o legislativní úpravě problematiky kybernetické kriminality. V závěru teoretické části jsou popsány jednotlivé kybernetické útoky, které jsou označovány jako kyberteroristické. Poslední část práce analyzuje výsledky dotazníkového šetření.

ABSTRACT

CHÝLEK, J.: *Cyber terrorism and attacks againt information technology: Bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2017. 59 p. Supervisor: RNDr. Růžena Ferebauerová

Key words: cyberterrorism, cybernetic attack, cyberspace, information technology, hacker

The bachelor's thesis deals with the issue of cyber-terrorism and cyberspace. The first part summarizes the information and concepts of cyberspace, terrorism and cyber-terrorism and focuses more on cyberspace, its definition, division and development. This part also analyzes the definition of terrorism and compares it with the definition of cyber-terrorism. The next part addresses the types of tools and attacks against information technology and deals with hacker issues. It describes their development and division according to their motivation and is followed by a part dealing with the legislative regulation of the issue of cybercrime. At the end of the theoretical part are described individual cyber attacks, which are referred to as cyber-terrorism. The last part analyzes the results of the questionnaire survey.

Obsah

Úvod 8
1 Cíl a metodika bakalářské práce 9
2 Základní vymezení 10
2.1 Kyberprostor 10
2.2 Terorismus 14
2.3 Kyberterorismus 15
3 Útoky na informační technologie 18
3.1 Nástroje pro kybernetické útoky 19
3.1.1 Prolamovače 19
3.1.2 Spyware 19
3.1.3 Viry 20
3.1.4 Červi 20
3.1.5 Rootkity 21
3.1.6 Trojské koně 21
3.1.7 Distribuované odepření služby 21
3.1.8 Přesměrovávače a Defacement 22
3.1.9 Nástroje průzkumu sítě 22
3.2 Hackeři a Crackeři 23
4 Legislativní úprava 26
4.1 Mezinárodní právní úprava 26
4.2 Právní úprava České republiky 28
5 Kazuistika 33
5.1 Výbuch transsibiřského plynovodu 1982 33
5.2 Následky incidentu v Bělehradě 1999 - 2001 34
5.3 Kybernetický útok na Estonsko 2007 35
5.4 Gruzie 2008 37
5.5 Stuxnet 2010 38

5.6 Flame 2012 38
5.7 Současnost 39
6 Praktická část 41
6.1 Metody a cíle výzkumu a stanovení hypotéz 41
6.2 Výsledky dotazníkového šetření 42
6.3 Ověření hypotéz 48
Závěr 50
Seznam použitých zdrojů 52
Seznam zkratek 56
Seznam tabulek a grafů 57
Přílohy 58

Úvod

Využívání kyberprostoru má celosvětový růst a výjimkou není ani Česká republika. Úroveň využívání internetu běžnými uživateli je srovnatelná s ostatními státy vyspělého světa. Pozadu není ani digitalizace výrobních procedur a státní správy. Ekonomika vyspělého světa 21. století je na využívání kyberprostoru přímo závislá a chod kteréhokoliv státu by výpadek tohoto komunikačního prostředí mohl ochromit. S překotným vývojem technologií vzrůstá efektivita moderních států, ale i jejich závislost. Tato závislost neuniká pozornosti různých zájmových skupin, které se jí snaží využít k ovlivnění svého profitu, či ke způsobení škod konkurenci. Střety těchto skupin, států, zpravodajských služeb a teroristických organizací vyvolávají v prostředí kyberprostoru regulérní válku. Je to skrytá kybernetická válka a jednotlivé strany konfliktu se snaží zahladit stopy po svých aktivitách. Někteří naopak propagují své úspěchy veřejně. Snaží se tak vyvolat strach a ovlivnit veřejné mínění. Mezi ty patří i teroristické organizace.

Hrozba kyberterorismu a jeho vnímání veřejností je důležité pro přípravu účinných opatření, kdy se jedná nejen o technická opatření, ale i úpravu právního rámce pro zajištění bezpečnosti informačních technologií.

1 Cíl a metodika bakalářské práce

Hlavní cíl bakalářské práce je zaměřen na definici kyberterorismu v kyberprostoru. V souvislosti s definicí pojmu kyberterorismu jsou rozebrány i jednotlivé nástroje používané ke kybernetickým útokům, proti informačním technologiím a význam pojmu hacker. Dále se práce zaměřuje na rozbor kyberteroristických útoků známých z historie a legislativní úpravu problematiky.

Informace a podklady pro dosažení těchto cílů byly čerpány z literárních a internetových zdrojů. Zdroje byly zkoumány metodou rešerše a komparace. Ke zjištění právního rámce ochrany kybernetického prostoru byly použity platné právní předpisy České republiky.

Metodou kvantitativního výzkumu a analýzou výstupu z dotazníkového šetření bylo zjišťováno povědomí o hrozbách útoků proti informačním technologiím a kyberterorismu.

Práce je rozdělena na teoretickou a praktickou část v celkově šesti kapitolách. První kapitola shrnuje cíle a metodiku bakalářské práce. Ve druhé a třetí kapitole jsou popsány jednotlivé definice kyberterorismu, kyberprostoru a jednotlivé druhy nejčastěji používaných útoků a jejich nástrojů.

Ve čtvrté kapitole je popsána právní úprava kybernetické bezpečnosti platná v České republice. Pátá kapitola věnuje pozornost jednotlivým kybernetickým útokům, které jsou dle dostupných zdrojů považovány za akty kyberterorismu. Šestá kapitola, praktická část práce, obsahuje vyhodnocení dotazníkového šetření, na základě zpracovaného dotazníku ve strukturované formě s uzavřenými otázkami.

2 Základní vymezení

V současnosti si již nelze představit fungování vyspělých států bez informačních technologií. Tyto jsou stále více provázány se všemi aspekty fungování státu a lidské činnosti. S častějším využíváním informačních technologií a rozšiřováním dosahu kybernetického prostoru souvisí i nárůst rizik. Tyto se už neomezují pouze na finanční zisk a dokazování schopností zkušených hackerů. Stále větší nebezpečí představují politicky a mocensky motivované útoky proti informačním technologiím. V dnešní době jsme stále častěji svědky kybernetických útoků, ze kterých jsou obviňováni hackeři zastupující vzájemně znesvářené státy a útoky samotné odrážejí konflikty na politické scéně. Předmětem těchto útoků bývá často zisk utajovaných informací, které mohou ovlivnit veřejné mínění, zdiskreditovat současnou vládu a změnit volební preference. Mnohem rizikovějším typem útoku je však takzvaný kyberterorismus. Předmětem útoku kyberterorismu jsou základní systémy, jejichž vyřazení může ohrozit lidské životy. Jejich účelem je způsobit co největší škody na lidských životech a zasít strach mezi civilním obyvatelstvem.

2.1 Kyberprostor

Pokud máme pochopit kyberteroristické útoky, je zapotřebí určit prostor ve kterém k těmto útokům dochází. Kyberprostor z původního znění, v anglickém jazyce cyberspace, je složením slov cyber odvozeném od řeckého slova kybernétes (kormidelník) a space (prostor).

Tento termín použil poprvé americký spisovatel sci- fi William Gibson v roce 1982 ve své povídce Burning Chrome. Následně tento termín rozvinul v románu Neuromancer, kde je zmíněna i první definice kyberprostoru: „*konsensuální halucinace každý den prožívaná miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky, grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat“*[1]

[1]KUŽEL, S. Kybernetická kriminalita od hackerů ke kybernetickým válkám. In *Business It*. [online]. [cit. 2017–04-30]. Dostupné z WWW: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php>

Pojem kyberprostoru vytyčený Gibsonem časem přešel z kyberpunkové komunity do technického světa a ujal se ve světě jedniček a nul. Definice kyberprostoru se začaly upřesňovat a jednou ze základních se stala definice Johna Barlowa, zakladatele Elektronik Frontier Foundation. Ten považuje za kyberprostor nejen počítačové sítě, ale i všechny telekomunikační sítě. Do kybernetického prostoru tedy mohou patřit i intranetové sítě, virtuální herní prostředí a sítě mobilních operátorů.[2]

Takto zkrácená a technicky pojatá definice Barlowa však nevypovídá o všem, co chtěl sdělit svojí „Deklarací nezávislosti kyberprostoru" z roku 1996. V té píše o kyberprostoru jako o přírodním jevu, který roste činností operátorů. Brání se zásahu vlád, kdy tyto vyzývá, aby nezasahovaly do kyberprostoru, který je svobodným prostorem a nesmí být omezován. Označuje ho za prostor sestávající se z transakcí, vztahů a myšlenek, kde může kdokoliv projevit svoje přesvědčení svobodně, beze strachu z následku a bez předsudků k jeho rase, vojenské síle či ekonomické moci. Zároveň odmítá omezení kyberprostoru zákony, kdy Barlow poukazuje na to, že je nehmotný a zákony se na něj nemohou vztahovat. „*Vaše právní koncepty majetku, projevu, totožnosti, pohybu a kontextu se na nás nevztahují. Všechny jsou založené na hmotě, a tady žádná hmota není. Naše identity nemají tělesné schránky, takže na rozdíl od vás nemůžeme zjednat pořádek pomocí fyzického násilí. Věříme, že naše zřízení se vyvine z mravů, osvíceného osobního zájmu a veřejného prospěchu. Naše identity mohou být rozeseté do spousty vašich právních řádů. Všechny naše dílčí kultury budou obecně uznávat jen jediný zákon, Zlaté pravidlo. Doufáme, že naše vlastní řešení problémů budeme moci vybudovat na jeho základě. Jenže nemůžeme přijmout řešení, která se nám snažíte vnutit.*" Svojí deklaraci pak zakončuje označením kyberprostoru jako civilizací mysli a vyjadřuje touhu, aby byla civilizovanější a lidštější než svět, který utvořily vlády světa.[3]

Tato deklarace vyjadřuje názor značného množství pokročilejších uživatelů internetu, kteří kyberprostor vnímají jako prostor svobody a nekonečných možností. Ač je tato deklarace již přes dvacet let stará, stále vyjadřuje aktuální střety mezi hackerskou komunitou a snahou sledování a omezování kyberprostoru. Příkladem může být hnutí Anonymous, které je veřejně známé svým bojem za svobodu internetu. V tomto boji

[2] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 17
[3] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 43 - 45

neváhá použít útoků proti informačním technologiím, jejichž popisu bude věnována pozornost v kapitole o útocích na informační technologie.

Kyberprostor tedy lze vnímat jako moderní nástroj komunikace a přenosu informací za pomoci nejmodernějších technologií výpočetní techniky. Kyberprostor je pro mnohé ideálem svobodného prostoru pro vyjádření svých názorů.

Kyberprostor je decentralizovaný, globální a poskytuje obrovské množství informací. A to chtěné i nechtěné, včetně záměrných dezinformací a hoaxů. *„Snaží se svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem.“*[4]

Do kyberprostoru je zapojena polovina světové populace, přičemž většina těchto uživatelů má jedno společné a to požadavek na co nejrychlejší přenos dat a spolehlivý přístup k síti. To jakou cestou se k datům dostane a jakou část sítě navštíví je druhotné. Kyberprostor se takto rozděluje do tří částí:[5]

Surface web je ten, který všichni dobře známe. Je dostupný klasickými webovými prohlížeči a je takto určen pro nejširší veřejnost. Jeho obsah je indexovaný a je možné ho vyhledat prostřednictvím prohlížeče. Zabírá asi 4 % obsahu kyberprostoru.

Deep web je tvořen intranetovými sítěmi, databázemi a informačními systémy, které nejsou běžně dostupné. Obsahuje neindexovaný obsah, který nelze běžným prohlížečem vyhledat. Celkově Deep web zahrnuje zbylých 96 % obsahu kyberprostoru. Nejedná se však o samostatný systém. Využívá stejné infrastruktury a systémů. Součástí Deep webu je takzvaný Darknet, nebo také Dark web.

Dark web je příkladem nezávislosti internetu. Jeho obsah je neregulovaný a zcela svobodný. K obsahu se může uživatel dostat za použití speciálního webového prohlížeče, jako je kupříkladu Tor Browser.[6] Kromě možnosti zcela svobodného pohybu v tomto kyberprostoru, ale přináší i svoji temnou stránku, kterou je například dětská pornografie, obchod s kradenými daty a malwarem. Na darknetu je možné online zakoupit prakticky cokoliv od drog až po zbraně. Příkladem takového obchodu byla Silk

[4] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 88
[5] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 46 - 51
[6] NUTIL, P. *Darknet, aneb cesta do hlubin internetu.* Kurzy [online]. 2015 [cit. 2017–05-04]. Dostupné z WWW: <http://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu/>

road, kde mohl kdokoliv pod anonymním účtem a s dostatkem Bitcoinů zakoupit vše na co si vzpomněl. Silk road byla v roce 2013 při zásahu FBI zavřena. Stejným způsobem skončily i další weby jako například Carder planet.[7]

K pochopení kyberprostoru je kromě definice důležitá i jeho historie. Začátek kyberprostoru a celosvětové sítě se začal psát v roce 1946 v Pensylvánii. Zde byl zkonstruován vůbec první sálový počítač s označením ENIAC. Jednalo se o velmi nákladný přístroj, ke kterému měla přístup pouze speciálně proškolená obsluha. Přesto se začal postupně rozšiřovat do dalších společností v USA.[8]

Poté co byl vytvořen nástroj, přišla na řadu myšlenka. Tou bylo vytvoření počítačové sítě, která by spojovala vojenské, strategické, akademické a vládní počítače. Základní vlastností této sítě měla být schopnost odolat útokům jaderného charakteru. Díky rozdělení sítě do vzájemně rovnocenných uzlů, bez centrálního řízení, se podařilo vyhovět požadované odolnosti. V říjnu roku 1969 byla takto zprovozněna síť Arpanet. Od této chvíle již nic nebránilo rozvoji kyberprostoru, který z původní sítě, skládající se ze čtyř uzlů univerzit v USA, vyrostl až do současných rozměrů. Za tu dobu prošel mnoha změnami, vznikl domain name system, systém IP adres a Arpanet nahradil internet s www.[9]

Nejnovější vývoj kyberprostoru se rozšiřuje za hranice běžných koncových zařízení. Současnost je označována jako doba průmyslové revoluce 4.0. Efektivita výroby se zvyšuje zapojením výrobních linek do kyberprostoru. Tato revoluce zahrnuje nejen průmysl, ale i běžné domácnosti, kde se do kyberprostoru připojuje domácí „chytrá“ elektronika. Tento trend se nazývá internet věcí. V loňském roce bylo k internetu věcí připojeno 6,4 miliard zařízení. V nadcházejících třech letech má jejich počet stoupnout, až na 50 miliard zařízení. Internet věcí bude ovládat nejen domácnosti, ale i infrastrukturu měst a kupříkladu jejich osvětlení. Dle Tomeše, je velkým nebezpečím nízká ochrana zařízení. Síť zavirovaných zařízení byla již v minulosti použita pro útok zahlcením internetových stránek, které pod vlivem tohoto útoku spadly.[10]

[7] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 46 - 51
[8] MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. s. 20
[9] PROCHÁZKA, D. *První kroky s internetem*, Praha: Grada Publishing, 2012. s. 12
[10] TOMEŠ, M. Průmysl prochází změnou jako nikdy předtím, říká autor knihy o internetu věcí, E15 [online]. 2017 [cit. 2017–06-04]. Dostupné z WWW: <http://e-svet.e15.cz/it-byznys/prumysl-prochazi-zmenou-jako-nikdy-predtim-rika-autor-knihy-o-internetu-veci-1333263>

2.2 Terorismus

Terorismus je jedno z nejvíce skloňovaných slov dnešní doby. Současné ohrožení Evropy náboženským terorismem dává tomuto pojmu reálné obrysy. Do většího povědomí se terorismus dostal spolu s útoky 11. září 2001 a následnou reakcí USA. Tehdy vyhlášená válka proti terorismu přetrvává dodnes a obyvatelé Evropy zjišťují, že teroristické útoky jsou nyní součástí jejich života. Pro poznání terorismu je potřeba hledět nejen na použité prostředky, ale i na jeho příčiny a účel. Definice terorismu tyto jednotlivé body popisují.

Jedna z definic je uvedena na stránkách ministerstva vnitra České republiky, kdy popisuje terorismus jako: „*Organizované použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím mají být splněny politické, náboženské nebo ideologické požadavky jak ve vnitrostátním, tak v mezinárodním měřítku*“[11]

V podobném smyslu je terorismus popisován i v odborné literatuře. *„Terorismus je třeba chápat jako útok na jistoty demokracie a na základní práva občanů např. právo na bezpečnost, život a další.*“[12] Podle Eichlerovy definice se stát stává předmětem útoku a vydírání. Účelem je manipulace s veřejným míněním, navodit atmosféru strachu, destabilizovat stát, snížit jeho věrohodnost a autoritu. Zároveň cílí na vyvolání reakce, která je v zájmu útočníka. Jedná se o změnu vnitřní, nebo zahraniční politiky. Za hlavní taktiku je považováno násilí, strach a komunikace s veřejností prostřednictvím poselství. Charakteristiku politického terorismu popisuje Eichler jako metodu prosazování politických cílů za použití násilí. Jejím primárním cílem je dosažení určitého zamýšleného psychického efektu. Tento má svým rozsahem významně překročit okruh přímých obětí či svědků útoku. Důležité jsou především politické důsledky, než samotný důsledek násilné akce. Hlavní částí dopadu teroristického útoku je moment zastrašování a terorizování cílového publika. Nejedná se ale o jedinou součást a není nezbytné, aby byla hlavní.[13]

[11] Pojmy – terorismus. Mvcr.cz [online]. 2017 [cit. 2017–05-30]. Dostupné z WWW: <http://www.mvcr.cz/clanek/pojmy-terorismus.aspx>
[12] PIKNA, B. *Mezinárodní terorismus a bezpečnost Evropské unie,* Praha: Linde, 2006, s. 35
[13] PAVLÍKOVÁ, M. Estonsko – Ruský incident v kontextu kyberterorismu, *Global Politics* [online]. [cit. 2017–06-04]. Dostupné z WWW: <http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu>

2.3 Kyberterorismus

Kyberterorismus spojuje pojmy kyberprostoru a terorismu. Ideál svobody v kyberprostoru zneužívají teroristické organizace pro svoje působení. Internet je pro ně dostatečně širokým působištěm, kde mohou skrývat finanční, strategické a koordinační akce. Teroristé nepůsobí pouze skrytě, ale kyberprostor využívají ke své propagaci, kterou je například sdílení záznamů z útoků, či poprav zajatců. Snaha využití kyberprostoru k podnikání útoků, které svým dopadem naplňují charakteristiku teroristického útoku, je aktuálním tématem. Pojem kyberterorismu rozebírá ve svém díle Jirovský, který zde doplňuje nejčastěji citovanou definici kyberterorismu. Kyberterorismus je konvergencí kyberprostoru a terorismu. „*Je obecně chápán jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů. K této definici pak doplňuje, že se citovaný útok musí odrazit v násilí proti jedinci nebo společnosti, nebo musí způsobit dostatečnou škodu na to, aby budil strach. V tomto smyslu jsou za akty kyberterorismu považovány útoky proti kritické infrastruktuře a útoky, které nenarušují klíčové služby obvykle pokládány za akty kyberterorismu nejsou.“*[14]

Jirovský dále uvádí různé druhy útoků, které motivací neodpovídají uvedené definici, ale svým dopadem ano. V tomto se však nevyhraňuje k označení takovýchto útoků za kyberteroristické, jak ve svém článku Konceptualizace kyberterorismu uvádí Jakub Drmola.[15] Stejně jako v případě terorismu je i kyberterorismus definován na stránkách Ministerstva vnitra. „*Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů („informační elektronické síťové struktury“)“*[16] Pojem kyberterorismu je uveden i ve slovníku kybernetické bezpečnosti. *„Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či*

[14] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 130 - 131

[15] DRMOLA, J. *Konceptualizace kyberterorismu,* Vojenské rozhledy [online]. 2013 [cit. 2017–06-04]. Dostupné z WWW: <http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu>

[16] Pojmy – Kybernetický terorismus - kyberterorismus. Mvcr.cz [online]. 2017 [cit. 2017–06-04]. Dostupné z WWW: <http://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx>

neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků.“[17]

Rozborem jednotlivých definic se zaobírá Drmola. Podrobněji rozebírá jednotlivé znaky kyberterorismu, kdy za cíl kyberteroristického útoku považuje politickou změnu a ideologickou propagandu než finanční profit, či přímé oslabení vojenských kapacit protivníka. Za jisté výjimky z tohoto pravidla považuje kriminální a psychopatologický terorismus. Dále zmiňuje, že důležitou charakteristikou je také možnost rozlišit takzvané cílové publikum od přímé oběti. *„Oběť kyberteroristického útoku je pouze prostředníkem, který má obvykle skrze zastrašení přenést poselství cílovému publiku. Od toho je následně očekávána a vyžadována nějaká akce či naopak absence akce, což je vyvoláno intenzivním strachem. Často zmiňovaná je role médií a snaha teroristů dosáhnout co nejširšího obecenstva skrze ochotná média.“*[18] U kyberterorismu se často setkáváme s tím, že se útočníci snaží svůj útok zakrýt a co nejvíce utajit. Publicita útoku je nežádoucí a podle Drmoly jsou takto utajované útoky mimo definici kyberterorismu. U kybernetické kriminality je utajení běžnou praxí, neboť není v zájmu útočníků odhalit bezpečnostní mezeru, natož svoji identitu. Terorismus v kyberprostoru naráží na úskalí kyberprostoru, kde je utajení tajemstvím úspěchu. Vyloučením cílového obecenstva a zamezením psychologického dopadu na širší veřejnost se aktivity teroristické organizace mohou vymanit z běžných definic. Pravý účinek zastrašení a přinucení k jednání je možný pouze tehdy, je-li přítomna hrozba, že dojde k útokům dalším. Dalším úskalím kyberprostoru je jeho samotná nehmotná podoba. Klasický teroristický útok se vyznačuje svojí násilností, která má šokovat širokou veřejnost. To je v prostředí kyberprostoru velmi obtížné, tedy útoky bývají zaměřeny spíše na ekonomické subjekty, vládní a zpravodajské internetové stránky s cílem způsobit vysoké ekonomické škody. Následným cílem je stejně jako u teroristického útoku ztráta důvěry ve vládu, či případná reakce vlády dle požadavků útočníka. Útok by měl ale stále splňovat vyvolání strachu z hrozby dalšího útoku. *„Kyberterorista tedy musí přesvědčit členy cílového publika, že nebude-li mu vyhověno, může být příští přímou obětí kdokoliv z nich. Útoky by také měly být součástí jakési souvislé kampaně sledující nějaký deklarovaný cíl. Pokud se jedná o jednorázovou akci,*

[17] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 71

[18] DRMOLA, J. *Konceptualizace kyberterorismu*, Vojenské rozhledy [online]. 2013 [cit. 2017–06-04]. Dostupné z WWW: <http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu>

na kterou útočník nemá možnost či zájem navázat, je tím značně zmenšena motivace publika vyhovět jeho požadavkům.“ [19]

[19] DRMOLA, J. *Konceptualizace kyberterorismu*, Vojenské rozhledy [online]. 2013 [cit. 2017–06-04]. Dostupné z WWW: <http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu>

3 Útoky na informační technologie

Jako útoky proti informačním technologiím se dají označit útoky za použití softwaru, hardwaru nebo přímého sociálního inženýrství. Pod pojmem sociálního inženýrství si můžeme představit případ, kdy zaměstnanec nebo bývalý zaměstnanec s přístupem k informačním technologiím je kompromitován útočníkem.[20] *„Jedná se o způsob manipulace lidí za účelem provedení určité akce, nebo získání určité informace.“*[21] Takováto osoba může nevědomky či cíleně předat citlivé informace útočníkovi. Někdy může dokonce použít upravený hardware k usnadnění útoku. Zaměstnanci se však stávají aktéry útoků i bez využívání sociálního inženýrství. Častým důvodem napadení firemního softwaru může být neopatrnost zaměstnanců, kteří otevřením přílohy spamu, či návštěvou nezabezpečené stránky, zanesou do firemního serveru malware.[22] FBI odhaduje podíl útoků proti informačním technologiím se zapojením vnitřních nepřátel na 80% z celkového objemu. Jako insider, tedy člověk zevnitř, je označován nejen zaměstnanec, ale i osoba, která se nějakým způsobem dostala fyzicky k cíli. Často se jedná o nespokojené zaměstnance, kteří úmyslně využijí svého přístupu k citlivým informacím nebo k spravování samotné firemní sítě. Takovýto nespokojený zaměstnanec může napáchat obrovské škody zničením dat nebo zcizením citlivých informací, které následně poskytne konkurenci.[23]

Jako příklad lze uvést případ Vitka Bodena, bývalého zaměstnance Australské firmy Hunter Watertech. Ještě jako zaměstnanec pomáhal s instalací dálkově ovládaného systému odpadních vod Maroochy shire v Austrálii. Po propuštění z firmy se za pomoci vysílačky a odcizeného laptopu naboural do systému řízení nádrže odpadních vod a do krajiny vypustil 800.000 litrů znečištěné vody. Za to byl odsouzen ke dvěma letům vězení a uhrazení vzniklé škody.[24]

---

[20] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004. s. 153 - 154

[21] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 107

[22] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 195 - 199

[23] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 114 - 127

[24] WEISS, J. *Maroochy water services case study,* Computer security division, Computer security resource center, [online]. 2008 [cit. 2017–06-04]. Dostupné z WWW: <http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf>

3.1 Nástroje pro kybernetické útoky

K softwarovým útokům a k útokům s použitím upraveného hardwaru jsou využívány různé speciální programy. Jedná se ve většině případů o volně sdílené programy, které na web umisťují samotní tvůrci v rámci hackerské komunity. Tento škodlivý software se v angličtině nazývá malware a může mít mnoho různých podob. Jeho názvosloví se liší dle funkce, kterou vykonává. Malware bývá často programován komplexně, kdy zahrnuje více funkcí. Záměrně je uváděna ta část programů, která může být využita při kyberteroristických útocích.

3.1.1 Prolamovače

Prolamovače se používají k prolamování hesel, jeden z nejstarších malwarů. Jejich účel je zřejmý a to prolomení ochrany či autorizace. V případě, že je tato ochrana prováděna statickým heslem, je možné použít prolamovač. Ten generuje kombinace znaků dle nastavení útočníka. I v případě použití prolamovače je důležité sociální inženýrství. Informace o uživateli, který heslo vytvořil, může zúžit okruh možných hesel. Prolamovač tedy generuje hesla, až do chvíle kdy narazí na správné. Správné heslo je následně odesláno útočníkovi. V případě neznalosti bližších informací k cíli, jsou použity dva základní druhy útoku. Slovníkové útoky používají známá slova z vlastní databáze. Útok hrubou silou postupně generuje všechny možné kombinace. Použití prolamovačů připadá v úvahu u autorizací bez automatické blokace, kde se po určitém počtu chybných zadání účet zablokuje. Dobu práce prolamovače lze odhadnout podle typů hesla. U čtyř velkých, nebo malých písmen je doba prolomení několik sekund. Oproti tomu na prolomení hesla, které se skládá z deseti velkých a malých písmen a číslic v libovolné kombinaci, je zapotřebí až 26984 let.[25]

3.1.2 Spyware

Spyware je špionážním malwarem, který je využíván k tajnému získávání dat o chodu počítače. Sleduje činnost uživatele a vzniklá data odesílá útočníkovi, který z něj získává potřebné informace.[26]

Spyware je často užíván i na základě souhlasu uživatele v souvislosti s cílenou reklamou. Jedná se o velice nebezpečnou a rozšířenou formu malwaru, která je pro

[25] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 62 - 63
[26] PETROWSKI, T. *Bezpečí na internetu pro všechny,* Liberec: Dialog, 2014. s. 35 - 36

napadeného uživatele velmi nebezpečná. Komplexní spyware může využívat funkci Traceru a sledovat tak pohyb cílového zařízení s GPS lokátorem. Zároveň sledovat provoz webového prohlížeče a za pomoci key loggeru ukládat historii stisku klávesnice. Za použití těchto nástrojů je pak snadné zjistit přístupové heslo, nebo důležité informace, které uživatel napíše.[27]

Podobnou špionáž provádí skenery, které slouží pro zjištění otevřených portů počítače. Skenují služby, které na počítači probíhají a zjišťují základní informace o operačním systému a jeho nechráněných místech. Informace o detekci skeneru je často předzvěstí nadcházejícího útoku. Podobně sniffery zachycují kompletní síťovou komunikaci u špatně zabezpečené sítě. Sniffer analyzuje celý datový tok a snaží se z něj získat užitečné informace.[28]

3.1.3 Viry

Název tohoto malwaru není zvolen náhodně. Stejně jako virus chřipky, potřebuje i počítačový vir svého hostitele. Napadá soubory a dokumenty, odkud se šíří dál na další hostitele. V 90. letech měly viry primárně destrukční vlastnosti, v současné době se viry snaží skrýt svoji činnost, rozšiřují se a stahují do napadeného systému další nežádoucí obsah. Typickým znakem je, že k jejich šíření není zapotřebí zásahu uživatele. Napadení virem lze bránit aktualizovaným antivirovým programem. Viry se dělí dle druhů napadených programů, tedy jejich nositelů, například boot viry, či makro viry.[29]

3.1.4 Červi

Červi jsou škodlivé programy, které nepotřebují k svému šíření hostitele. Šíří se zpravidla samostatně, prostřednictvím sítí a napadají připojená zařízení. Z napadených zařízení se pak kopírují a prostřednictvím sítě se šíří dále. Na rozdíl od virů umí sami hledat bezpečnostní mezery a pronikat přes ně. Jedná se tedy o malware, který je schopen vykonávat více funkcí.[30] Červ může být například naprogramován jako logická bomba, která spustí až po splnění předem daných podmínek. Do té doby se pouze skrytě šíří. Po daném podnětu, například spuštění webového prohlížeče, dojde k její aktivaci.[31]

---

[27] POŽÁR, J. *Informační bezpečnost,* Plzeň: Aleš Čeněk, 2005, s. 216
[28] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 64 - 65
[29] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 207 - 208
[30] PETROWSKI, T. *Bezpečí na internetu pro všechny,* Liberec: Dialog, 2014. s. 33
[31] DUNNIGAN, J. *Bojiště zítřka: Tváří v tvář hrozbě kybernetického terorismu,* Praha: Baronet, 2004, s.336

3.1.5 Rootkity

Takzvané rootkity jsou využívány k zahlazení stop po napadení systému. Jedná se o soubor technik pro skrývání činností prováděných na operačním systému. Program typu rootkit mění vlastnosti součástí systému, aplikací, nebo celého operačního programu.[32] Tyto programy a techniky jsou schopny skrýt malware v napadeném systému a maskovat vybrané běžící procesy.[33] Rootkit je často skryt v menších programech a rozlišuje se na systémové (napadá jádro systému a modifikuje ho) a aplikační (modifikuje konfiguraci aplikací). Je zaměřen především na ochranné programy, jejichž úkolem je odstraňovat nebezpečný software, typicky antivirové programy. Použitím rootkitu brání malware před zásahem antivirového programu.[34]

3.1.6 Trojské koně

Jedná se o počítačové programy, jejichž účelem není samostatné šíření bez zásahu uživatele. Trojský kůň může být samostatný program, nebo součást jiného programu. Takový program se tváří jako neškodný systémový nástroj, až do jeho aktivace. Trojský kůň může po aktivaci sledovat provoz počítačového systému, kopírovat a mazat data. Vyspělé typy trojského koně mohou otevřít porty počítače a připravit tak počítačový systém k dalšímu útoku. Trojské koně mohou taktéž využívat komunikační aplikace jako je ICQ. V kombinaci s trojským koněm bývají často používány skenery.[35] Nejstarší trojské koně využívali uživatelé kyberprostoru spíše jako žert a drobný vandalismus. Postupem času se ale začaly stávat nebezpečnějšími a ničily údaje a programy.[36] Trojské koně šíří útočníci jako součást freewarových programů nebo je vkládají do ukradených autorských děl, která dají volně ke stažení.[37]

3.1.7 Distribuované odepření služby

Dosud uváděné programy a viry mohou umožnit napadení počítače zombie programem. Uživatel jeho působení nepostřehne, ale na pozadí počítače program komunikuje s útočníkem, který ho tam umístil. Díky zombie programu získá útočník

[32] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 65
[33] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 99
[34] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 209
[35] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 209
[36] DUNNIGAN, J. *Bojiště zítřka: Tváří v tvář hrozbě kybernetického terorismu,* Praha: Baronet, 2004, s.339
[37] PETROWSKI, T. *Bezpečí na internetu pro všechny,* Liberec: Dialog, 2014. s. 38

kontrolu nad napadeným počítačem.[38] Útočník si postupně buduje síť napadených zařízení, takzvaných botnetů. Botnet je síť tisíců infikovaných počítačů, kterou ovládá jediný cracker.[39] Ty pak může použít k distribuovanému útoku proti cílovému systému. Síť botnetů zašle systému dotazy, které zahltí a nakonec zcela přetíží provoz. Důsledkem je zpomalení služby, nebo úplné vyřazení dostupnosti webových stránek.[40]

3.1.8 Přesměrovávače a Defacement

Přesměrovávače jsou programy, které umožní přesměrovat uživatele na jiné stránky, než chtěl původně navštívit. Stránky, na které je uživatel přesměrován, obsahují škodlivý malware, který se tímto způsobem instaluje do počítače. Defacement je oproti tomu průnik přímo na server, který má za cíl pozměnit jeho obsah. Nejedná se o skrytý útok, ale naopak se snaží o co největší zviditelnění. Jeho účinkem je vyvolání nedůvěry a strachu z užívání napadeného serveru ale i zviditelnění názorů a ideologie útočníka.[41]

3.1.9 Nástroje průzkumu sítě

Ve výčtu nelze, jako vůbec základní nástroj, opomenout nástroje průzkumu sítě. Před použitím malwaru je v přípravné fázi před útokem potřeba prozkoumat cíl. Mnoho důležitých informací získávají útočníci z otevřených zdrojů, ke kterým se lze dostat za pomoci obyčejného prohlížeče. Přes webové prohlížeče se tak útočník může dozvědět podrobnosti o majiteli firmy, jeho zaměstnancích, ale i obchodních partnerech a funkci společnosti. Kromě samotného nástroje je zapotřebí využití sociálního inženýrství a skládání kusých informací do logických celků. Výsledkem může být poměrně celistvý obraz cíle, který útočníkovi usnadní jeho další snažení. Analýza webových stránek nezůstává u viditelného obsahu, dalším důležitým zdrojem informací je zdrojový kód stránky. Takto může zjistit jméno tvůrce stránek, datum a čas vytvoření, nebo informace o dalších stránkách. Základní informací zdrojového kódu je nástroj, který byl použit pro vytvoření kódu.[42]

---

[38] DUNNIGAN, J. *Bojiště zítřka: Tváří v tvář hrozbě kybernetického terorismu,* Praha: Baronet, 2004, s.340

[39] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 107

[40] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 295 - 299

[41] Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Ministerstvo vnitra* [online]. [cit. 2017–06-04]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>

[42] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 67

3.2 Hackeři a Crackeři

"Toto je teď náš svět. Svět elektronů a spínačů, krása baudu. Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily „šmelinářským hltounům“, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, aby jsme věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci. Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho co říkají a co si myslí a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny... konec konců, všichni jsme stejní.“[43]

Hackerův manifest sepsal 8. ledna 1986 Loyd Balneknship vystupující pod přezdívkou The Mentor, krátce po svém zatčení. Od jeho sepsání je brán jako základní průvodce etikou a motivací hackerů.[44] Hackeři jsou v souvislosti s mediální prezentací vnímáni veřejností jako zločinci, jejichž motivací jsou krádeže a rozesílání virů. Pojem hacker a hacking v dnešním slova smyslu vešel ve známost na začátku sedmdesátých let při vzniku takzvaného blue boxu. U jeho zrodu stála skupinka, která se nazývala phreakers. Jednalo se o skupinku v okruhu jistého Johna Dreapera, do které mimo jiné patřili zakladatelé firmy Apple, Steve Jobs a Steve Wozniak. Tito využili akustického ovládání telefonní sítě a za použití dětské píšťalky a krabičky od cereálií simulovali příkaz, který jim umožňoval volání zdarma. Skutečný rozvoj započal v osmdesátých letech s rozvojem Bulletin Board Systémů, systémů, které umožňují vzdálené připojení s možností čerpání dat z počítačů připojených k síti za použití telefonní linky. V tomto období byli součástí hackerské komunity téměř výhradně studenti s přístupem do univerzitních počítačových center. Hackerské skupiny se zabývaly převážně prolamováním hesel a zjišťováním slabin systémů. Zjištěné informace sdílely a používaly k záplatování a k opravám vad v systému. Jejich hlavní zásadou bylo volné

[43] DOLEJŠÍ, K. 1986 Hackerův manifest. In: *Britské listy* [online]. [cit. 2017–06-04]. Dostupné z: <http://blisty.cz/art/14662.html>
[44] DOLEJŠÍ, K. 1986 Hackerův manifest. In: *Britské listy* [online]. [cit. 2017–06-04]. Dostupné z: <http://blisty.cz/art/14662.html>

sdílení informací. S rozvojem webových prohlížečů a sdílením hackerských nástrojů se možnosti útočit proti informačním technologiím rozšířily i mezi širší veřejnost.[45]

Hackerův manifest sdílí podobnou myšlenku jako deklarace nezávislosti kyberprostoru. Základ manifestu a celkové myšlenky hackera je absolutní svoboda jednání v kyberprostoru. Hacker neuznává soukromé vlastnictví, cenzuru či zákonné omezování prostředí internetu. Jedná se o zručnou osobu, která umí pronikat do chráněných systémů. Cílem nemusí být získání nebo zničení informací, ale spíše prokázání vlastních kvalit v komunitě a sobě samotnému. Důležité je překonání ochrany systému.[46] Čím těžší a složitější systém se podaří hackerovi překonat, tím více uznání sklízí v komunitě. Jde především o prokazování zdatnosti v jejich oboru. Hacking bývá jednou z nejdůležitějších součástí jejich života, kdy udržování dostatečných znalostí pro nabourávání ochranných systémů a programování vlastního malwaru zabere mnoho času. Získaná data nebo programy využívají často pouze pro svoji potřebu nebo pro potřebu svých přátel.[47] I u samotného zrodu internetu byli hackeři - programátoři, kteří opracovávali systém, řešili softwarové problémy, dokud nebyly vyřešeny. Kdo tedy jsou zločinci zmiňovaní ve zpravodajstvích, kteří se nabourají například do internetového bankovnictví soukromým osobám za účelem převodu peněz? Tito jsou nazýváni hackery. Uvnitř hackerské komunity se ale názvosloví podstatně více rozlišuje. Zatímco zmíněný hacker nabourává systémy, pro vlastní zdokonalení a prokázání schopností, cracker využívá své schopnosti pro kriminální jednání.[48]

Mimo toto rozdělení se vžilo označení dobrých a zlých hackerů s odkazem na staré westernové filmy. Tak jako ve filmech se hackerská komunita dělí na kladné hrdiny s bílým kloboukem white-hat a zloduchy s černým black-hat. Zatímco white hats jsou hackeři, kteří dodržují hackerskou etiku a často pracují pro firmy, kde pomáhají se zabezpečením systémů, provádí zkušební útoky na slabá místa a v případě nálezu provádí opravu systému. White hats vytváří skupiny hackerů jako je tiger team, nebo sneakers. Black hats oproti tomu působí s cílem napadnout systém a prolomit ochranné prvky systému bez souhlasu uživatele. Získané výhody narušení systému pak získávají sami pro sebe, nebo pro organizaci, která je najme. Nejznámější skupinou je H4H a její

[45] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 47 - 56
[46] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004. s. 154 - 155
[47] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 51
[48] DUNNIGAN, J. *Bojiště zítřka: Tváří v tvář hrozbě kybernetického terorismu,* Praha: Baronet, 2004, s.335 - 336

služby si může objednat kdokoliv s dostatkem prostředků. Služby black hats využívá organizovaný zločin i extremistické skupiny. Rozdělení na černou a bílou nemohlo postihnout všechny hackery a tak vznikl pojem grey hats. Šedé klobouky se pohybují na hraně mezi oběma skupinami. Často se jedná o začínající hackery, kteří se prozatím nerozhodli, na kterou stranu se dají.[49] Zároveň zahrnují hackery, kteří již za sebou mají řadu zkušeností a útoky veřejně upozorňují na zranitelnost systémů.[50]

Z pohledu kyberterorismu připadá v úvahu skupina black hat hackerů, kdy existuje možnost, že se některý z nich nechá najmout teroristickou organizací. Mezi hackery se však nacházejí i tací, kteří by se kyberteroristického činu mohli dopustit i bez vize finančního zisku. Craktivista, nebo také hacktivista je označení pro ideologické hackery. Jedná se o členy politicky, nebo nábožensky založených skupin. Svojí činnost v kyberprostoru směřují k prosazování svých politických a ideologických cílů. Může se jednat i o příznivce extremistických skupin či náboženských radikálů.[51]

Hackerská komunita pojmenovala nebezpečnou část osob, která podniká útoky na počítačové systémy, jsou jimi script kiddies, lamers, loosers a n00bs. Jedná se o osoby s minimálními technickými dovednostmi, které pouze využívají vytvořené nástroje druhých, sami žádné programy nevytvářejí a útoky provádí bez ohledu na následky. Naštěstí nástroje, ke kterým se dostanou, jsou často již v databázích antivirových programů. A tak jejich útoky dopadají spíše na špatně chráněné a neaktualizované systémy. Přesto i takovýto útok mívá často zničující následky.[52]

[49] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 55
[50] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 107
[51] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 56
[52] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 56

4 Legislativní úprava

Kybernetická kriminalita a její právní úprava je neustále měnícím se prostředím. Stále se objevují nové hrozby a legislativa se na ně snaží reagovat. Mezinárodní úmluvy a samotná právní úprava České republiky se snaží zabraňovat nově vzniklým druhům protiprávní činnosti. Vznik právních předpisů je zdlouhavý proces a nestačí překotnému vývoji technologií. Proto je nesnadné některé nelegitimní jednání definovat a zařadit do platné právní úpravy.

Kolouch[53] popisuje kybernetickou kriminalitu, jako kriminalitu kde jsou informační a telekomunikační technologie užity jako prostředek trestného činu nebo jsou cílem útoku, přičemž tento útok je trestným činem a prostředky jsou užity nebo zneužity v informačním, systémovém, programovém či komunikačním prostředí. Zároveň pak uvádí, že toto vymezení nelze brát doslovně. Současné rozšíření informačních technologií rozšiřuje užití informačních technologií i na jiné trestné činy jako je například podněcování nebo schvalování trestného činu. Tedy krom jeho pozitivního vymezení, uvádí potřebu vymezit i činy, které mezi kybernetickou kriminalitu řadit nelze.

Na kriminalitu související s pokročilými technologiemi lze pohlížet široce jako na jakoukoliv činnost s prvky výpočetní techniky. Nebo také užším vymezením jako výhradně na činy spáchané proti informačním technologiím.[54]

4.1 Mezinárodní právní úprava

Vývoj technologií k ochraně dat a informačních systémů je předmětem mnoha vědních výzkumů, kdy do tohoto vývoje jsou vkládány nemalé finanční prostředky. Pro efektivní využití těchto prostředků je zapotřebí přesné vymezení, kam až může ochrana dat sahat a zároveň vymezit předmět ochrany. Kvůli rozdílnosti právních úprav jednotlivých států, by byla takováto ochrana značně nejednotná. Efektivní ochranu tedy

[53] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 36
[54] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 65

nelze uplatňovat bez nadnárodního právního rámce a to nejen v rámci Evropské unie, ale i celosvětově.[55]

Jako jeden z prvních dokumentů mezinárodního práva, který se zaobírá problematikou kybernetické kriminality, byl Manuál OSN o prevenci a kontrole trestných činů spojených s počítači z roku 1990.[56]

Nejvýznamnější dokument týkající se kybernetické kriminality je v současné době Úmluva Rady Evropy č. 185 o kyberkriminalitě, která byla schválena Výborem ministrů rady Evropy v roce 2001. V platnost vstoupila 1. července 2004 a jejím účelem je sjednocení právních norem jednotlivých států a zlepšení postihu mezinárodní kybernetické kriminality. Česká republika úmluvu podepsala v roce 2005, ale ratifikována byla až v roce 2013.[57] Úmluva stanovuje členským státům povinnost implementovat do národních právních řádů nástroje, které umožní postih definovaných trestných činů. Úmluva se skládá se z preambule a 48 článků a vytváří právní rámec pro sjednocení postupu proti pachatelům trestných činů. Vymezuje používané pojmy, upravuje trestní právo hmotné, trestní právo procesní a soudní pravomoc, nastavuje zásady mezinárodní spolupráce. Definované druhy kybernetických útoků rozděluje do čtyř skupin: trestné činy proti utajování a dostupnosti počítačových dat a systémů, trestné činy související s obsahem, počítači a porušováním autorských práv. V roce 2003 byl přijat dodatkový protokol č. 189, který doplnil trestné činy související s šířením materiálu s rasistickým či xenofobním obsahem.[58]

Úmluvou snaha Evropské unie o sjednocení právní úpravy neskončila. Jako další prostředky, kterým se právní úpravy sjednocují, jsou využívány především rámcová rozhodnutí, nařízení a směrnice. Kolouch[59] jen mezi ty nejvýznamnější řadí celkem 26 různých dokumentů.

V souvislosti s Estonsko Ruským konfliktem nelze opomenout Talinský manuál mezinárodního práva použitelný pro kybernetickou válku, který rozebírá aplikaci mezinárodního práva na kybernetickou válku. Tento dokument vznikal v letech 2009 –

[55] KOLOUCH, J. *Trestněprávní ochrana před kybernetickou kriminalitou*, Praha: Policejní akademie, 2013. s. 65
[56] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 331
[57] GŘIVNA, T. Úmluva o kybernetické kriminalitě. In: *Europen* [online]. [cit. 2017–06-08]. Dostupné z: <http://www.europen.cz/Proceedings/32/Umluva%20o%20kybernetickе%20kriminalite.pdf>
[58] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 332
[59] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 335 - 337

2012 ve spolupráci expertní skupiny kybernetické obrany NATO v reakci na události v Estonsku.[60]

4.2 Právní úprava České republiky

Kyberprostor nemá vlastní právní úpravu ve smyslu základních práv daných zákonem. V přístupu ke kyberprostoru je třeba využít obecně závazné právní normy. Virtuální svět není od toho reálného odtržený a je třeba implementovat základní práva i na tento prostor. Technické řešení kyberprostoru má ale globální povahu a tak se často střetává s lokálním právem. Internet není právně subjektivní, nemá majitele ani sídlo. Subjekty právních vztahů zde představují samotní uživatelé.[61] Základní práva jsou zakotvena v Listině základních práv a svobod, ústavní zákon číslo 2/1993 Sb.., kdy v souvislosti s právy v kyberprostoru lze jako stěžejní úpravu uvést několik článků Listiny:

Článek10

(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Článek 11

(1) Každý má právo vlastnit majetek. Vlastnické právo všech vlastníků má stejný zákonný obsah a ochranu. Dědění se zaručuje.

Článek 13

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou

[60] FLÍDR, T. Mezinárodní právo kyberprostoru a Talinský manuál, In: *Kyberbezpečnost*, [online]. [cit. 2017–06-08]. Dostupné z: < https://www.kyberbezpecnost.cz/?p=198>

[61] KOLOUCH, J. *Cybercrime*, Praha: CZ.NIC, 2016. s. 90 - 92

případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.[62]

Právo na ochranu soukromí a majetku je dále řešena v prostředcích soukromého práva, kde je stěžejní občanský zákoník číslo 89/2012 Sb.. Tento upravuje soukromé právo a jeho ochranu.[63] V případě kybernetických útoků a kyberterorismu bude narušení uvedených práv natolik zásadní, že k ochraně dotčených práv bude užito trestního zákoníku č. 40/2009 Sb.., který v reakci na ratifikovanou úmluvu užívá aktuální terminologii a v souladu s ní se zaměřuje i na skutkové podstaty kybernetické kriminality. Trestné činy související s kybernetickým prostorem se nacházejí ve zvláštní části zákona. Aplikace prostředků informačních technologií při páchání trestných činů má široké pole působnosti od trestných činů proti životu a zdraví, až po trestné činy proti lidskosti, proti míru a válečné trestné činy. V případech kybernetických útoků, které mohou směřovat ke spáchání kyberteroristického činu, lze uvést pro příklad několik skutkových podstat uvedeného zákona.

§ 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

[62] ČESKO. Zákon č. 2/1993 Sb., Listina základních práv a svobod: In *Sbírka zákonů, Česká republika*. 1993, částka 1, s. 19 - 20. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426>.
[63] ČESKO. Zákon č. 89/2012 Sb., občanský zákoník: In *Sbírka zákonů, Česká republika*. 1993, částka 33, s. 1026- 1027. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=24084>

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

(1) Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.[64]

Z pohledu kyberterorismu je třeba zmínit i skutkovou podstatu teroristického útoku. Informační technologie jako prostředek zde přímo uvedeny nejsou. Tyto je třeba hledat jako cíl útoku. Tímto ustanovením zákona je chráněn samotný kyberprostor v podobě informačních systémů a komunikačních technologií. Zároveň si lze představit

[64] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 394 - 406. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.

útoku v kyberprostoru, který může závažně poškodit veřejná zařízení či přerušit dodávky vody a energie.

§ 311 Teroristický útok

(1) *Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla,*

a) *provede útok ohrožující život nebo zdraví člověka s cílem způsobit smrt nebo těžkou újmu na zdraví,*

b) *zmocní se rukojmí nebo provede únos,*

c) *zničí nebo poškodí ve větší míře veřejné zařízení, dopravní nebo telekomunikační systém, včetně informačního systému, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, veřejné prostranství nebo majetek s cílem ohrozit tím lidské životy, bezpečnost uvedeného zařízení, systému nebo prostranství anebo vydat majetek v nebezpečí škody velkého rozsahu,*

d) *naruší nebo přeruší dodávku vody, elektrické energie nebo jiného základního přírodního zdroje s cílem ohrozit tím lidské životy nebo vydat majetek v nebezpečí škody velkého rozsahu,*

e) *zmocní se letadla, lodi, jiného prostředku osobní či nákladní dopravy nebo pevné plošiny na pevninské mělčině, nebo nad takovým dopravním prostředkem nebo pevnou plošinou vykonává kontrolu, anebo zničí nebo vážně poškodí navigační zařízení nebo ve větším rozsahu zasahuje do jeho provozu nebo sdělí důležitou nepravdivou informaci, čímž ohrozí život nebo zdraví lidí, bezpečnost takového dopravního prostředku anebo vydá majetek v nebezpečí škody velkého rozsahu,*

f) *nedovoleně vyrábí nebo jinak získá, přechovává, dováží, přepravuje, vyváží či jinak dodává nebo užije výbušninu, jadernou, biologickou, chemickou nebo jinou zbraň, anebo provádí nedovolený výzkum a vývoj jaderné, biologické, chemické nebo jiné zbraně nebo bojového prostředku nebo výbušniny zakázané zákonem nebo mezinárodní smlouvou, nebo*

g) *vydá lidi v obecné nebezpečí smrti nebo těžké újmy na zdraví nebo cizí majetek v nebezpečí škody velkého rozsahu tím, že způsobí požár nebo povodeň nebo škodlivý účinek výbušnin, plynu, elektřiny nebo jiných podobně nebezpečných látek nebo sil nebo se dopustí jiného podobného nebezpečného jednání, nebo takové obecné nebezpečí zvýší nebo ztíží jeho odvrácení nebo zmírnění.*[65]

Kromě trestního zákoníku je od 1. 1. 2015 účinný zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Základní myšlenkou tohoto zákona je zvýšení bezpečnosti kybernetického prostoru a jeho cílem je ochrana nejdůležitějších částí infrastruktury, které jsou důležité pro chod státu a jejíž narušení by vedlo k poškození nebo ohrožení zájmů České republiky. Zákon neřeší obecně veškerou kybernetickou kriminalitu, ale právě prevenci útoků proti infrastruktuře a způsob reakce na hrozby a řešení incidentů. Zároveň zavádí do legislativy nové pojmy jako kybernetický prostor, kritická informační infrastruktura. V zákoně byl definován národní a vládní CERT (computer emergency response team) a jejich úkoly při reakci na kybernetické bezpečnostní události a incidenty.[66] Zároveň zákon přesně definuje co je bezpečnostní událost a incident:

§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

(1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.[67]

Zákon o kybernetické bezpečnosti přinesl praktický nástroj pro reakci na kybernetické útoky. Je tak dalším stupněm v legislativním procesu sjednocování postupů jednotlivých signatářů Úmluvy o kyberkriminalitě.

---

[65] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 426. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.
[66] HROMADA, M., *Kybernetická bezpečnost*, Praha: Powerprint, s. 10 - 25
[67] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In *Sbírka zákonů, Česká republika*. 2014, částka 75, s. 1928. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231>.

5 Kazuistika

Společným znakem většiny z těchto útoků je účast státních organizací, politických aktivistů a hackerských hnutí jednotlivých států. Téměř vždy mají politické pozadí a často jim předcházely válečné nebo diplomatické konflikty mezi státy. Jedno má společné téměř každý z níže popisovaných případů, a to absenci odhalení konkrétního pachatele útoku. Zdroje vždy hovoří buď o domněnkách, které v příčinné souvislosti poukazují na politického oponenta napadeného státu, nebo na hackerskou skupinu, která se k činu přihlásila. Níže popsané případy často připomínají kybernetickou válku, průmyslovou špionáž či kontrašpionáž mezi různými mocnostmi. To neubírá na jejich značném dopadu, ale vyvolává otázku, zda lze takové útoky označit za útok teroristický.

5.1 Výbuch transsibiřského plynovodu 1982

Vůbec prvním případem, který je popisován jako kyberteroristický útok je uváděn případ Ruského transsibiřského plynovodu. V roce 1982 došlo k výbuchu přivaděče plynovodu z těžebního pole Urengoj do Čeljabinsku. Tehdejší Sovětský svaz výbuch přiznal, ale bližší informace nebyly nikdy sděleny. Výbuch je pak, zaznamenanou silou výbuchu tří kilotun TNT, označován jako největší nejaderný výbuch. Jako kyberteroristický útok je označován v díle At the Abyss spisovatelem Thomasem Reedem. Reed se ve své knize odkazuje na informace o kontrašpionáži prováděné agenty CIA, kdy agenti CIA v rámci zapojení do linie X předkládali Sovětskému svazu upravený software a hardware. Podle spekulací přiklánějící se ke kybernetickému útoku, měl být Sovětskému svazu podstrčen software ovládající SCADA systémy. Do tohoto softwaru byl vložen trojský kůň, který po spuštění systému narušil jeho chod a způsobil výbuch plynovodu.[68] Předávání upravených technologií přiznává samotná CIA ve zveřejněném dokumentu Farewell Dossier.[69]

[68] ERBEN, L. Příchod hackerů. In: *Root* [online]. [cit. 2017–06-04]. Dostupné z WWW: <http://www.root.cz/clanky/prichod-hackeru-zrod-kyberneticke-valky/>

[69] WEISS, G. W. The Farewell Dossier, In: *Central Inteligence Agency* [online]. [cit. 2017–06-04]. Dostupné z WWW: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm>

Žádným z aktérů studené války nikdy nebylo potvrzeno, že by se jednalo o útok, není tedy vyloučeno, že šlo o nehodu. Je však podezření, že šlo o cílený útok, za využití trojského koně uloženého v řídicím systému SCADA, který by byl oprávněně označován za kybernetický. Útok mohl být proveden zpravodajskou službou USA proti Sovětskému svazu v době studené války. Jednalo by se tedy spíše o součást války za použití kybernetických technologií, než o kyberteroristický útok.

5.2 Následky incidentu v Bělehradě 1999 - 2001

Během války v Kosovu bylo ze strany jugoslávských hackerů provedeno několik úspěšných útoků na webové stránky NATO. Největší vlna následovala po události, ke které došlo v únoru 1999. CIA v době války označila jediný cíl pro letecký útok. Mělo se jednat o federální ředitelství zásobování v Bělehradě. Označený cíl byl ve skutečnosti čínskou ambasádou a při zemřeli dva čínští novináři.[70] Následně začaly kybernetické útoky na webové stránky americké administrativy a zpravodajských serverů. Za původce je označovaná takzvaná Red hacker alliance, která vznikla na území Číny. Útoky protestního charakteru neměly vážnější dopady. S přihlédnutím k cílům útoku a jejich následkům lze tento útok označit spíše jako projev hacktivismu.[71] Útoky postupně ubíraly na síle, aby opět v roce 2001 nabraly na intenzitě po srážce amerického výzvědného letounu a čínské stíhačky. Americká posádka byla po nouzovém přistání zadržena. V následné vypjaté situaci začaly podnikat hackerské skupiny obou stran vzájemné útoky. Čínští hackerské skupiny Honker, Union of China a Chinese Red Guest Networka Security Technology Alliance podnikaly vytrvalé útoky. Vytvořen byl i server KILL_USA na kterém byla umístěna řada volně stažitelných programů k útokům na americké servery. V reakci na to vznikla obdobná stránka s názvem KILL_CHINA. Jirovský ve své knize označuje tento konflikt jako kybernetickou válku. Při tom upozorňuje na skutečnost, že přes rozsah útoků nebyl nikdo z obou stran odsouzen.[72]

[70] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 166
[71] ERBEN, L. Příchod hackerů. In: *Root* [online]. [cit. 2017–06-04]. Dostupné z WWW: <http://www.root.cz/clanky/prichod-hackeru-zrod-kyberneticke-valky/>
[72] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 166

5.3 Kybernetický útok na Estonsko 2007

Současný rozvoj digitálních technologií a jejich provázání na infrastruktury moderních států přináší vážná rizika. Napětí mezi státy a politické konflikty, které se v reálném světě projeví prohlášením či výzvou politického zastoupení jedné země vůči zástupcům země druhé, se může v digitálním prostředí strhnout v kybernetický konflikt. Příkladem je Estonský incident z jara roku 2007, při kterém pouhý přesun památníku v centru Tallinnu zapříčinil rozsáhlý kybernetický útok na státní, bankovní a zpravodajské servery. Příklad Estonského incidentu ukazuje jak stinnou stránku, kterou jsou finanční ztráty tohoto malého státu, tak i přínos, kterým je rozšíření povědomí o kybernetické bezpečnosti, zavedení a spolupráce národních bezpečnostních týmů, rozvoj legislativních a bezpečnostních opatření v rámci celé Evropské unie.

Estonsko se svou rozlohou a počtem obyvatel řadí mezi nejmenší státy Evropy, avšak v digitálním prostředí hraje významnou roli, kdy si v roce 2007 připsalo světové prvenství. Čtyři dny před zahájením parlamentních voleb, umožnilo voličům, v rámci experimentu, hlasování prostřednictvím Internetu. Tamní infrastruktura a dostupnost připojení na internet je jedna z nejlepších na světě. V roce 2006 Estonsko sestavilo tým zvaný CERT (Computer Emergency Response Team), jehož hlavním úkolem bylo reagovat na jakékoliv průniky do webových serverů Estonska. CERT začal sledovat internetový provoz jdoucí do země, přes ni i ven a vyhledávat abnormality a pokusy o průnik. V této době bylo Estonsko na vrcholu digitálního rozvoje, což bylo jeho obrovskou výhodou v souvislosti s událostmi roku 2007. [73]

Estonsko začalo v roce 2007 projednávat přesun sovětského válečného památníku z náměstí hlavního města Tallinnu, což vyvolalo negativní odezvu jak ruské menšiny obývající Estonsko, která ale tvoří téměř čtvrtinu obyvatelstva, tak z ruské strany. Nejdříve poklidné protesty se později změnily v násilné střety s policií, ke kterým došlo 27. 4. 2007. Politickou reakcí ruské strany byla jednání o nastavení možných sankcí vůči Estonsku. Zároveň v Rusku probíhaly protesty u Estonské ambasády, kdy došlo i k její krátkodobé blokaci. Tato reakce nijak nezměnily záměr odstranění památníku. V krátké časové návaznosti na tyto události se objevily tři týdny trvající kybernetické útoky. Útoky směřovaly na webové stránky estonské vlády, bank a médií. Mezi 27. a 29. dubnem 2007 probíhala první fáze útoku, která je nazývána „emocionální odezva“.

[73] GLENNY, M., *Temný trh, Kyberzloději, kyberpolicisté a vy,* Praha: Dokořán, 2013. s 155 - 156

Útoky směřovaly nejen proti webovým stránkám vládních stran, ale napadeny byly také zpravodajská média, která informovala o incidentech na ulicích spojených s přesunem památníku. Nejednalo se o nijak propracované útoky. I díky tomu nezpůsobila první vlna útoku zvlášť zásadní následky. Díky připravenosti týmu CERT, v souvislosti s nedávným průběhem voleb, pod vedením bývalého policejního důstojníka Hillera Aerelaida podařilo navýšit kapacity datových linek mířících do země a to za asistence ze zahraničí. S navýšením zejména pomohlo Finsko a Švédsko. Díky dobře nastavené spolupráci mezi vládou, policií, bankami a týmem CERT byl dopad útoku vcelku zanedbatelný, bez zásadních dopadů na ekonomiku. Po těchto začátcích došlo 3. 5. 2007 k masivnímu útoku. Cílem útoku byla Estonská banka Hansabank, proti které byl podniknut DDoS útok. Jednalo se o rozsáhlý botnet složený až z 80.000 počítačů, címž se podařilo vyřadit internetové bankovnictví. Hansabank ale na záložních serverech spustila náhradní přístup k bankovnictví, které tímto mohli klienti dále využívat.[74] Hansbank se podařilo udržet online bankovnictví funkční, druhé dvě nevětší banky tak úspěšné nebyly, útočníkům se podařilo jejich službu vyřadit.

Druhá fáze útoků byla označována jako „hlavní útok“. Oproti první fázi byla ta druhá lépe koordinovaná a více sofistikovaná. Od 30. dubna do 18. května byly napadány DNS (Domain name systém) servery, tedy servery doménových jmen. Ty překládají názvy domén na číselné IP adresy a zpět.[75] Tato fáze útoku měla více vln. První vlna začala 4. května, kdy se jednalo o DDoS útoky vůči různým webovým stránkám a DNS serverům za použití botnetů. Útoky se dařilo zakrývat využitím globálních botnetů, vedeným přes zahraniční servery a IP adresy. Následovala druhá vlna útoku v termínu od 9. do 11. května. Dne 9. května vychází výročí Dne vítězství nad nacismem. Vzhledem k významu dne v souvislosti s odstraněním památníku byly útoky očekávány a nakonec opravdu přišly. Jednalo se opět o masivní DDoS útoky, kterými se podařilo vyřadit celkem 58 převážně vládních stránek. Také bankovní servery zaznamenaly útoky od 9. do 11. května, kdy se klienti bank nemohli přihlásit dvě hodiny do systému. V té době se Estonská vláda rozhodla učinit radikální řešení, tedy odpojila zahraniční datové linky. DDoS útoky postupně ustávaly až 19. 5. 2007 zcela přestaly.[76]

[74] GLENNY, M., *Temný trh, Kyberzloději, kyberpolicisté a vy,* Praha: Dokořán, 2013. s 155
[75] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 107
[76] GLENNY, M., *Temný trh, Kyberzloději, kyberpolicisté a vy,* Praha: Dokořán, 2013. s 155 - 158

Z politického kontextu bylo zcela zřejmé, že za útoky stojí Rusko, nebo alespoň jeho občané. Moskva odmítla jakýkoliv podíl na útocích. Je samozřejmě možné, že vláda Ruské federace nebyla iniciátorem útoku, ale vzhledem k rozsahu útoku a způsobu kontroly internetového prostoru o útocích musela vláda vědět. Rusko nebylo nikdy označeno přímo za viníka- Estonské ministerstvo zahraničí uveřejnilo IP adresy, z kterých byl veden útok. Mezi nimi byly i IP adresy ruské vlády a prezidentské kanceláře. Mluvčí Kremlu Dmitrij Peskov, zcela popřel jakékoliv zapojení Ruska do tohoto kybernetického útoku, kdy poukázal na to, že IP adresy botnetu pocházely z celého světa a ne jen z Ruska. Podle výsledků vyšetřování byl nakonec původ útoku opravdu v Rusku, ale za hlavní útočníky byli označení ruští hacktivisti. To, že by byla do útoku zapojena Ruská vláda, se nepotvrdilo.[77]

5.4 Gruzie 2008

Válka o Jižní Osetii se projevila také na internetu. Mezi 19. – 20. červencem 2008 proběhla řada DDoS útoku proti gruzínským vládním webům. Tomuto útoku předcházelo šíření seznamu vládních webů na ruských diskuzních fórech. Mezi 9. – 10. srpnem pak došlo k mohutnému útoku, kterým se podařilo vyřadit prakticky veškeré gruzínské weby. Gruzie byla nucena požádat o pomoc zahraniční státy. Webové stránky velkých firem a státních orgánů byly přesunuty na zahraniční hosting, ale ani po tomto úkonu útoky nepřestaly. Na napadených stránkách gruzínského prezidenta Saakašviliho se objevila fotografie Adolfa Hitlera. Tento hosting byl umístěn v USA. Američtí hackeři následně prováděli odvetné útoky na webové stránky v Rusku. Útoky byly provedeny podobným způsobem jako výše popsaný případ Estonska, kdy ani zde se ruská strana k útokům nepřihlásila. Není jasné, jestli se na útoku podílela přímo ruská vláda, nebo se jednalo o haktivisty. Gruzínci se během konfliktu pokusili o odvetné útoky na zpravodajské weby v Rusku, ale jen s malými úspěchy. Po provedení útoku byli do Gruzie vysláni Estonští odborníci z CERT, aby navázali spolupráci mezi státy napadenými ruskými hackery.[78]

[77] PAVLÍKOVÁ, M. Estonsko – Ruský incident v kontextu kyberterorismu, *Global Politics* [online]. [cit. 2017–06-05]. Dostupné z WWW: <http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu>

[78] SEKERA, T. Kybernetické útoky: Rusko? – Gruzie a svět. In *mvcr.cz* [online]. [cit. 2017–06-05]. Dostupné z WWW: <www.mvcr.cz/soubor/zpravodajstvi-dokumenty-prezentace-spolecnosti-logica.aspx>

5.5 Stuxnet 2010

Dalším případem je napadení SCADA systémů ("Supervisory Control And Data Acquisition", tedy "dispečerské řízení a sběr dat") počítačovým červem Stuxnet. SCADA systémy jsou řídícím softwarem pro stěžejní průmyslovou výrobu, distribuční sítě vody, elektřiny a plynu, řízení dopravních sítí a komunikačních sítí.[79] Stuxnet byl objeven v roce 2010 běloruskou firmou VirusBlockada. Tento červ se zaměřoval na skryté přeprogramování SCADA systémů a převzetí kontroly, aniž by byl zaznamenán. Využitím chyby operačního systému Windows testoval, zda se nachází na počítači, na kterém je nainstalován řídicí software Siemens. Pokud tomu tak bylo, upravil software a skryl svoji činnost. Součástí Stuxnetu bylo připojení k internetovému serveru, kdy takto mohl předat informace a převzít příkazy.[80]

5.6 Flame 2012

Flame je modulární malware, který byl 28. 5. 2012 zjištěn a pojmenován ve vzájemné spolupráci MAHER center, CERT, Kasperky Lab a CrySyS Lab of the Budapest University of Technology and Economics. Dle vyjádření CrySyS Lab se jednalo o nejvíce komplexní malware s kterým se do té doby setkali. Tento malware se šířil prostřednictvím sítí a USB disků. Jednalo se o špionážní malware, který napadal počítače s operačním systémem Windows, kde byl schopen sledovat internetovou aktivitu, přehrávat a otvírat uložené soubory a snímat používání klávesnice. Mimo jiné se také napojoval na komunikační službu Skype a dokázal u napadeného zařízení pomocí Bluetooth stáhnout kontaktní údaje z dostupných zařízení. Na rozdíl od Stuxnetu se jednalo o špionážní malware, který za pomocí rootkitů skrýval svoji aktivitu. Informace stažené z napadených zařízení byly odesílané na vzdálené servery po celém světě, které se postupně měnily. Zaměřoval se pak převážně na stahování nákresů v PDF formátu a zpracovaných v AutoCadu. Flame dle zprávy Kasperky Lab napadal převážně vládní a univerzitní servery a soukromé počítače zemí blízkého východu. Celkem 65% napadených zařízení bylo v Izraeli, Egyptě, Saudské Arábii, Íránu, Libii, Sýrii a Libanonu. V roce 2012 vyšel ve Washington Post článek, který se

[79] JIRÁSEK, P. *Výkladový slovník kybernetické bezpečnosti,* Praha: Policejní akademie České republiky v Praze. 2015. s. 107

[80] BITTO, O. Stuxnet: virová předzvěst třetí světové?. In: *Živě* [online]. [cit. 2017–06-05]. Dostupné z WWW: <http://www.zive.cz/clanky/stuxnet-virova-predzvest-treti-svetove/sc-3-a-153951/default.aspx>

zaobíral verzí, že původcem útoku je U.S. National Security Agency, CIA a Izrael. Objevují se názory, že za útokem může stát i Čína. Dle zprávy Kasperky Lab, se Flame silně podobá Stuxnetu a může se jednat o jednotný útok za pomocí dvou odlišných malwarů. Skrytá špionážní povaha Flame mu na rozdíl od Stuxnetu umožnila delší působení a pozdější odhalení.[81]

5.7 Současnost

Faktem je, že útoky oficiálně označených teroristických skupin nejsou zmiňovány. Napadený stát může takovýto úspěšný útok záměrně zakrýt, aby nebyla zpochybněna jeho kybernetická bezpečnost. Ale pravděpodobnějším důvodem jsou spíše nedostupné technologie a především nedostatek útočníků s potřebnými znalostmi. Nejsou známy ani případy spolupráce black hat hackerů s těmito skupinami. Naopak jsou webové stránky teroristických skupin pravidelně napadány hackerskými skupinami v reakci na teroristické útoky v reálném světě. Příkladem může být rozsáhlý útok hackerské skupiny Anonymous na webové stránky Islámského státu po útocích v Paříži z roku 2015.[82]

V posledních letech dochází k radikalizaci potomků muslimských přistěhovalců v Evropě. Jedná se často o jedince s vysokoškolským vzděláním, kteří mohou mít rozsáhlé zkušenosti s informační technologií. Je tedy možný nástup využívání kyberprostoru teroristickými skupinami pro podnikání útoků. Útok může být podniknut čistě prostřednictvím kyberprostoru proti některému ze SCADA systémů. Napadení klíčových systémů může mít obrovské ekonomické důsledky a eventuální sekundární ztráty na životech. Takovýto útok je velmi obtížný a málo pravděpodobný, větší hrozbu představuje útok kombinovaný. Při tomto útoku by mohli teroristé použít konvenční útok v kombinaci s napadením serverů bezpečnostních služeb nebo zahlcením telekomunikačních linek, což by podpořilo vzniklý chaos a teoreticky zhoršilo efektivitu reakce bezpečnostních a záchranných složek. Částečnou útěchou může být fakt, že ani teroristické skupiny, které působí ve vyspělých státech Evropy, jako je ETA či IRA, nebyly doposud schopny dosáhnout těchto útoků.

[81] PINKAVA, J. Bezpečnostní střípky: „supermalware“ Flame odhalovány jsou stále nové vlastnosti. In: *Root* [online]. [cit. 2017–06-05]. Dostupné z: <http://www.root.cz/clanky/bezpecnostni-stripky-supermalware-flame-odhalovany-jsou-stale-nove-a-nove-vlastnosti>

[82] NOVINKY. Hnuti anonymous napadlo už přes 5500 účtů Islámského státu na twitteru. In: *Novinky* [online]. [cit. 2017–06-05]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/svet/386646-hnuti-anonymous-napadlo-uz-pres-5500-uctu-islamistu-na-twitteru.html>

Teroristické skupiny v současné době hojně využívají kyberprostor k vlastní prezentaci útoků a poprav zajatců pomocí webových stránek či profily na sociálních sítích. Tento prostor je taktéž hojně využíván k zveřejňování návodů na výrobu výbušnin, postupům k provedení útoků a verbování nových příznivců. Neopomenutelnou součástí je využívání komunikačních kanálů v kyberprostoru. Václav Jirovský ve své knize popisuje komunikaci Al – Kaidy, která využívala k předávání zpráv text skrytý ve volných bitech obrázků ve formátu jpg, které byly vystaveny na pornografických webových stránkách.[83]

[83] JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. s. 130 - 137

6 Praktická část

Výzkum praktické části bakalářské práce byl zaměřen na širokou veřejnost uživatelů informačních technologií ve věku od 14 let až po 60 let a více.

6.1 Metody a cíle výzkumu a stanovení hypotéz

Pro analýzu v praktické části bakalářské práce, byla zvolena metoda kvantitativního výzkumu. Tento byl proveden sběrem dat prostřednictvím online, anonymního dotazníku se záměrně uzavřenými otázkami ano – ne, díky kterým se musel respondent přiklonit k jednomu z tvrzení i v případě, že nemá o dané problematice hlubší znalosti. K dosažení cíle zapojení pouze aktivních uživatelů informačních technologií, byl využit pouze online dotazník.

Cílem výzkumu bylo zjištění názoru, případně domněnek široké veřejnosti na stav ohrožení kyberterorismem a připravenost České republiky bránit se takovému útoku. Dalším výstupem z dotazníkového šetření bylo zjištění ochoty omezení vlastní svobody v kyberprostoru pod záminkou vyšší bezpečnosti. Dle zjištění v teoretické části, byl jako jeden z hlavních nástrojů kyberteroristických útoků používán DDoS útok. V souvislosti s tím byla další část výzkumu zaměřena na otázky v souvislosti se základním zabezpečením informačních technologií a hrozbou zapojení nechráněných zařízení do botnetu.

Otázky dotazníku byly vytvořeny na základě tří stanovených hypotéz.

Hypotéza č. 1

Občané se cítí ohroženi kyberterorismem a nejsou přesvědčeni o schopnostech České republiky ubránit se této hrozbě.

Hypotéza č. 2

Občané nejsou ochotni připustit omezení vlastních práv, v souvislosti s bezpečnostními opatřeními.

Hypotéza č. 3

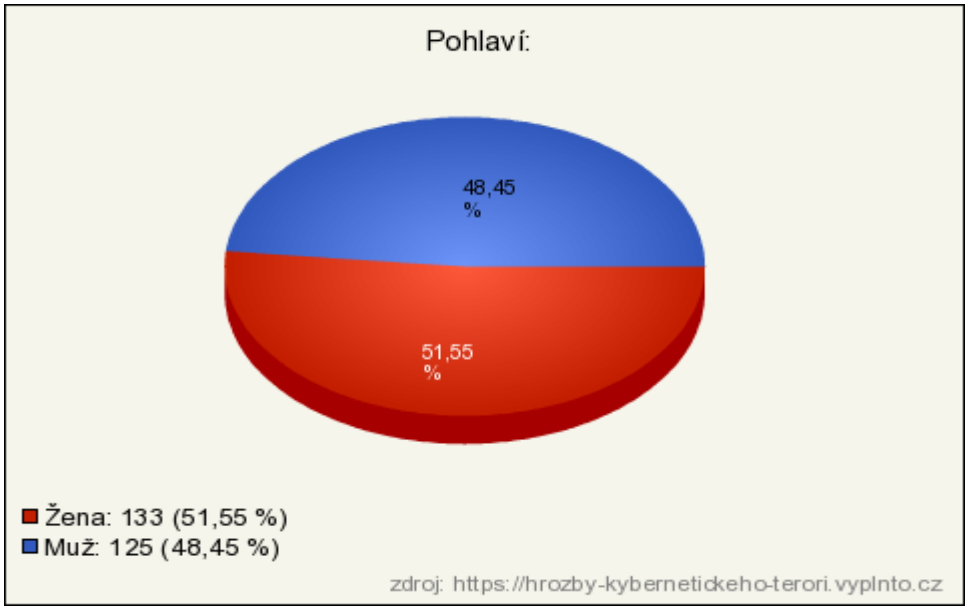
Občané chrání své počítače, ale zanedbávají ochranu mobilních zařízení a aktualizace systémů.

6.2 Výsledky dotazníkového šetření

Základní tři otázky zjišťovaly osobní údaje respondentů. V souvislosti s řešenou problematikou a způsobem šíření dotazníku byla ve výzkumu pouze minimálně zastoupena skupina 60 let a více. Dalších devět otázek bylo zaměřeno na cíle praktické části. Za pomoci analýzy závislosti odpovědí, bylo zjišťováno zastoupení skupin respondentů u jednotlivých otázek.

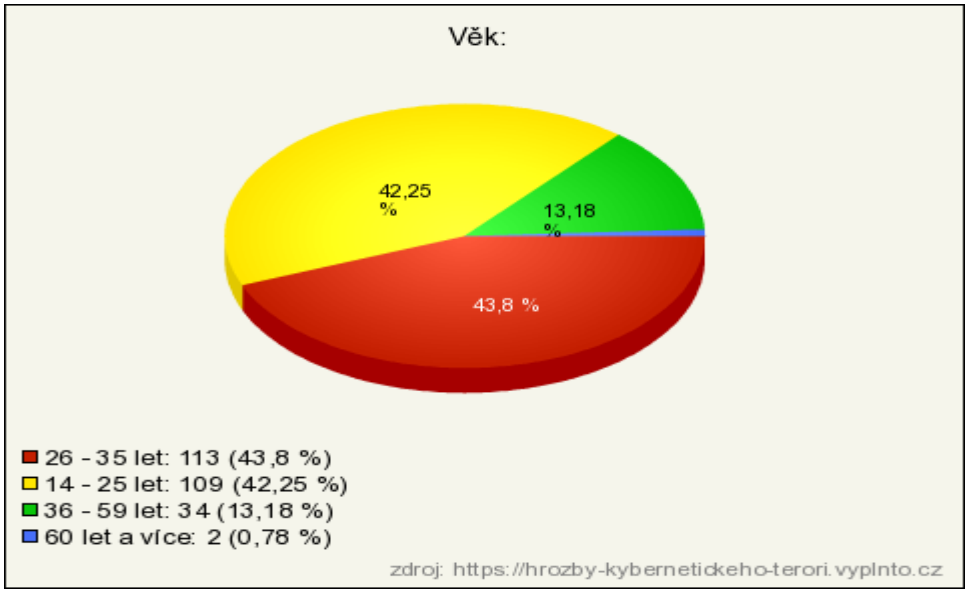
Graf č. 1 - Pohlaví

Žen účastnících se výzkumu bylo nepatrně více než mužů.



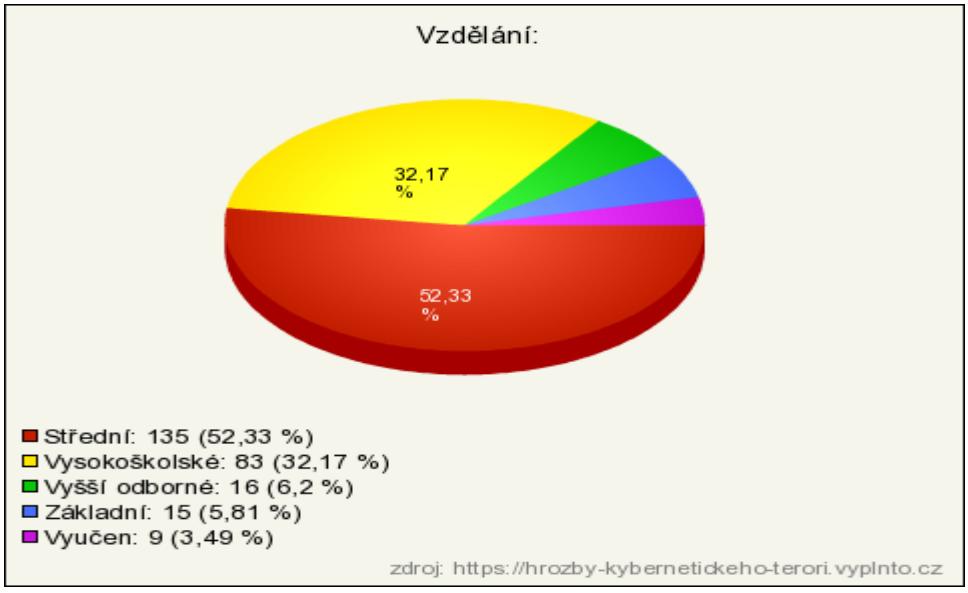
Graf č. 2 - Věk

Nejvyšší počet respondentů tvořila věková skupina 26 – 35 let s vyrovnaným zastoupením žen a mužů. Nepatrně méně respondentů spadalo do věkové skupiny 14 – 25 let, kde byly více zastoupeny ženy. Skupinu 36 – 59 let tvořil 13 % respondentů se srovnatelným zastoupením žen a mužů a pouze 2 repondenti ve věku 60 let a více.



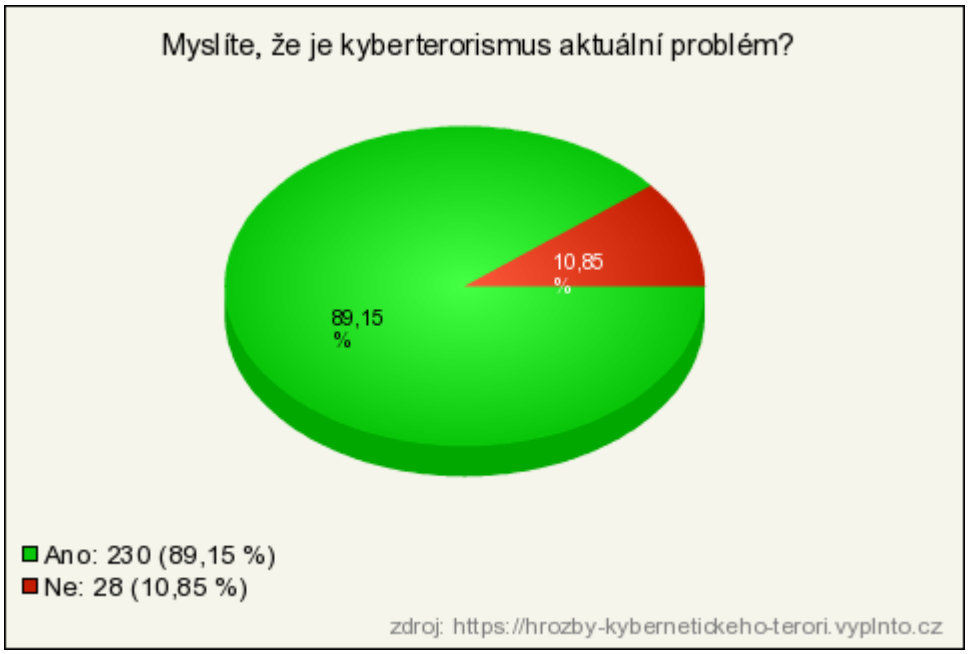
Graf č. 3 – Vzdělání

Dotazníkové šetření se zúčastnili respondenti všech stupňů dosaženého vzdělání. Více než polovinou tvořili středoškolsky vzdělaní, kteří spolu s respondenty se základním vzděláním tvořili většinu skupiny ve věku 14 – 25 let. Vysokoškolsky vzdělaní tvořili přes 32 % dotázaných. Necelých 15 % tvořily zbylé tři skupiny.



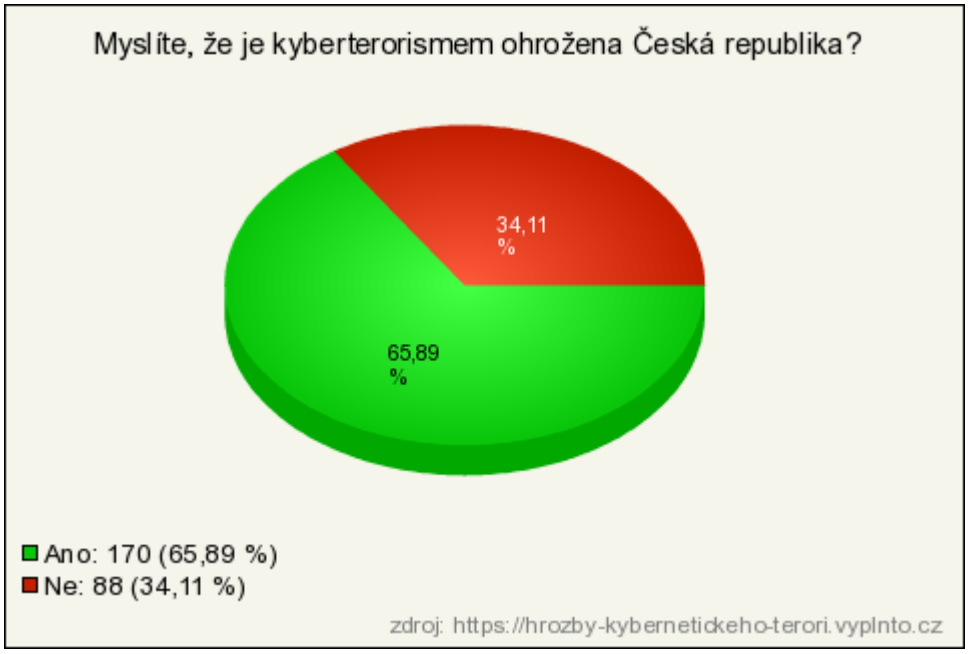
Graf č. 4 – Myslíte, že je kyberterorismus aktuální problém?

Většina dotázaných se přiklání k názoru, že se jedná o aktuální problém. Pouze necelých 11 % se domnívá, že tomu tak není. Jedná se z většiny o muže se středoškolským vzděláním.



Graf č. 5 – Myslíte, že je kyberterorismem ohrožena Česká republika?

Celých 34 % dotázaných si nemyslí, že je kyberterorismem ohrožena Česká republika. Stejně jako u minulého dotazu tvoří tuto skupinu spíše muži.

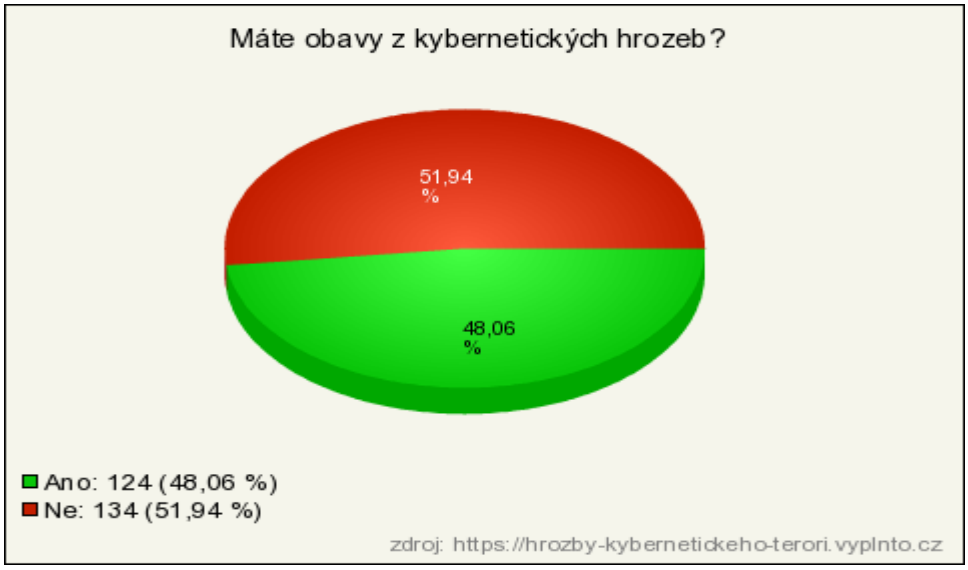


Graf č. 6 – Myslíte, že je Česká republika připravena čelit kybernetickým hrozbám?

Nedůvěru v připravenost České republiky vyjádřila většina respondentů. Větší důvěru projevují muži.

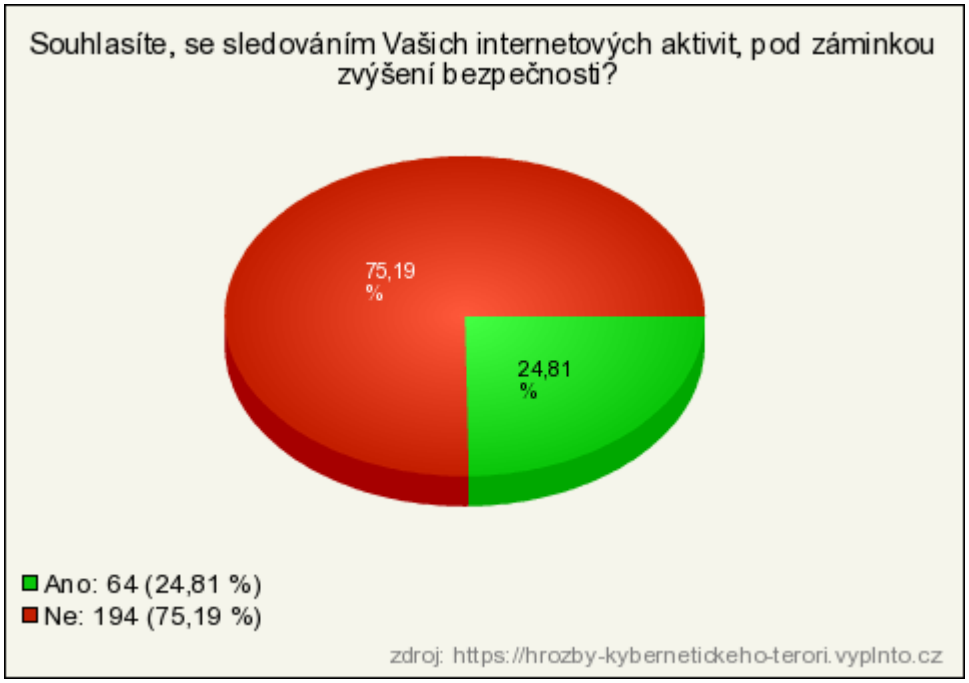
Graf č. 7 – Máte obavy z kybernetických hrozeb?

Více jak polovina respondentů sama nepociťuje obavy z kybernetických hrozeb. Rozdělení respondentů dle pohlaví, věku a vzdělání je u tohoto dotazu rovnoměrně rozděleno.



Graf č. 8 – Souhlasíte, se sledováním Vašich internetových aktivit, pod záminkou zvýšení bezpečnosti?

Tři čtvrtiny dotázaných odmítá omezení sledování jejich aktivit v kyberprostoru, přes výhody zvýšení bezpečnosti. Stejně jako u předchozího grafu je rozložení respondentů vyrovnané.

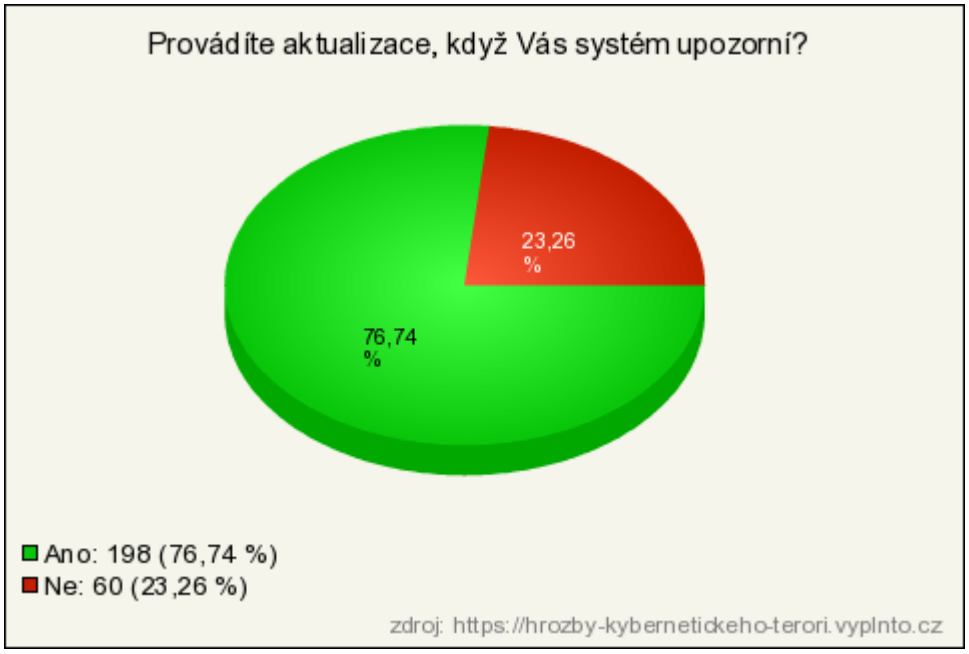


Graf č. 9 – Chráníte svůj počítač pomocí antivirového programu?

Naprostá většina respondentů má svůj počítač chráněn antivirem.

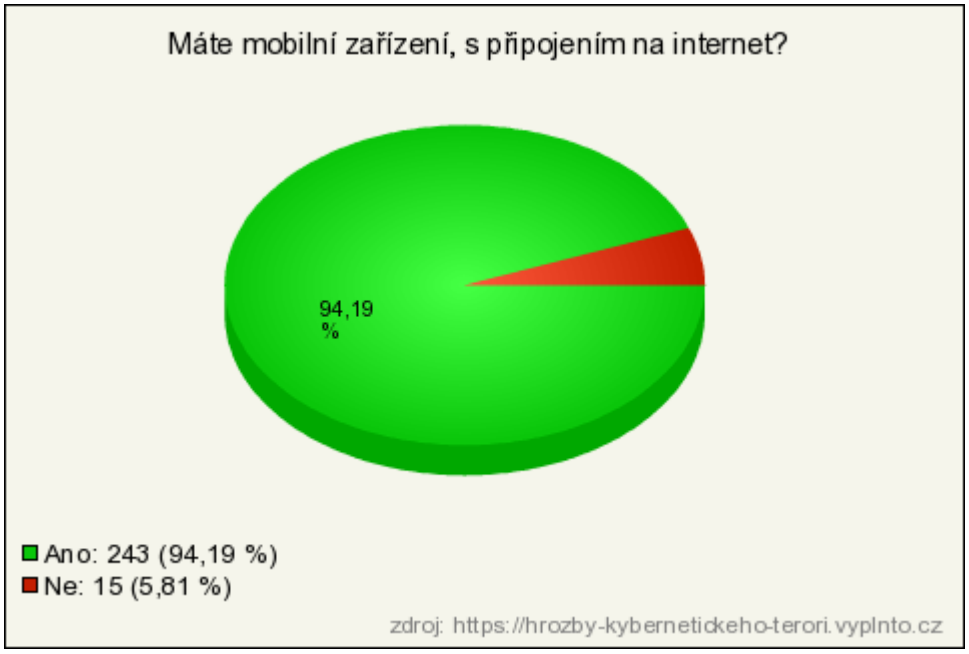
Graf č. 10 – Provádíte aktualizace, když Vás systém upozorní?

Provádění aktualizací na později nechávají převážně ženy.



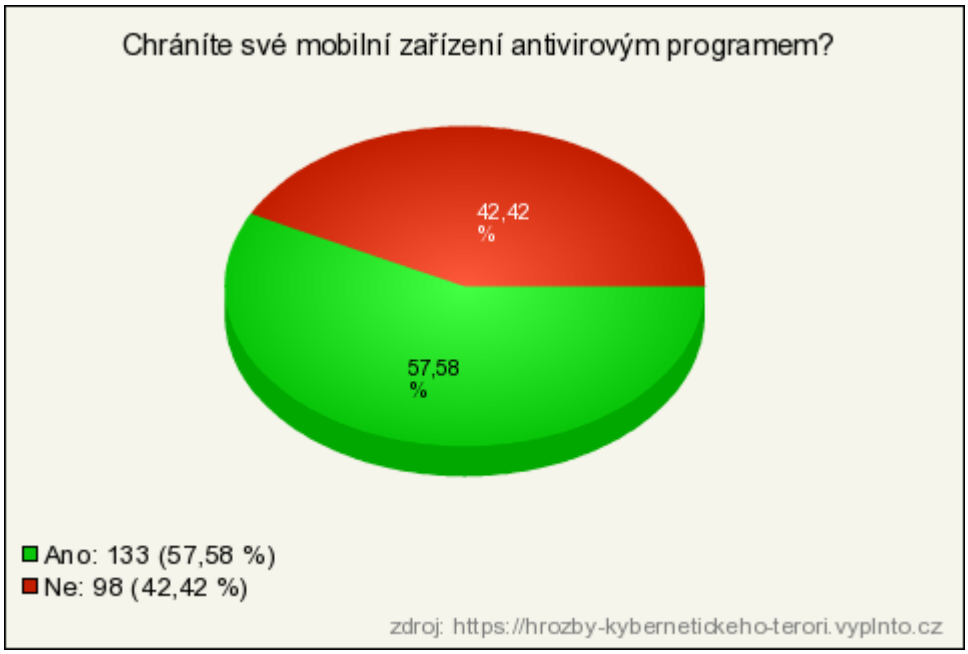
Graf č. 11 – Máte mobilní zařízení s připojením na internet?

Tímto mobilním zařízením disponují téměř všichni respondenti.



Graf č. 12 – Chráníte své mobilní zařízení antivirovým programem?

Až 98 respondentů nechává svůj mobilní telefon bez ochrany. U žen i mužů jsou výsledky srovnatelné. Nejvíce si svá mobilní zařízení chrání respondenti ve věku 36 – 59 let.



6.3 Ověření hypotéz

K vytvoření a vyhodnocení dotazníku bylo využito webu vyplnto.cz. Do výzkumu se přihlásilo celkem 258 respondentů z různých věkových skupin. Návratnost dotazníku dosahovala 83,6 %. Za účelem zpřístupnění dotazníku bylo využito sociálních sítí. Většinu respondentů se podařilo oslovit na sociální síti Facebook, kdy se jednalo o 95,5 % osob. Hlavní nárůst počtu vyplnění byl po zveřejnění dotazníku na facebookových stránkách věnovaných práci bezpečnostních sborů. Další respondenti se k dotazníku dostali přes web vyplnto.cz v 0,8 % případů, google.cz v 0,7 % případů a z nezjištěného odkazu v 2,6 % případů.

Hypotéza č. 1

Občané se cítí ohroženi kyberterorismem a nejsou přesvědčeni o schopnostech České republiky ubránit se této hrozbě.

Na základě otázek a grafů č. 4, 5, 6 a 7 byla hypotéza potvrzena. Otázka č. 7 ukázala, že přes vědomí hrozeb se samotní uživatelé kyberprostoru necítí příliš ohroženi. **Hypotéza verifikována.**

Hypotéza č. 2

Občané nejsou ochotni připustit omezení vlastních práv, v souvislosti s bezpečnostními opatřeními.

Na základě vyhodnocení otázky a grafu č. 8 se hypotéza potvrdila, kdy většina respondentů odmítá omezení vlastních svobod. **Hypotéza verifikována.**

Hypotéza č. 3

Občané chrání své počítače, ale zanedbávají ochranu mobilních zařízení a aktualizace systémů.

Vyhodnocením otázek a grafů č. 9, 10 a 12, bylo zjištěno, že většina respondentů chrání nejen svůj počítač, ale i mobilní zařízení. A zároveň provádí aktualizace systému, když je systém upozorní. **Hypotéza falzifikována**

Závěr

Cílem práce bylo objasnění pojmu kyberterorismu. Práce shrnuje popis kyberprostoru, od prvotní zmínky ve vědeckofantastické literatuře, přes deklaraci nezávislosti kyberprostoru, až po současné definice. Součástí je i exkurs do historie kyberprostoru a jeho dělení. Dále je popsán samotný terorismus a jeho definice. Popsáním těchto pojmů se podařilo připravit dostatečné povědomí pro pochopení pojmu kyberterorismu. Kyberterorismus je rozveden do několika pojmů a je rozebírána problematika terorismu v kyberprostoru. Výsledkem bylo zjištění, že kyberprostor má své vlastní zákonitosti, ve kterých nelze tvrdě uplatňovat definice terorismu. Kyberterorismus tedy nemusí vždy splňovat stejné znaky jako terorismus.

Kyberterorismus není pouze v teoretické rovině, ale má i své konkrétní nástroje a aktéry. Hlavní nástroje, které jsou využívány pro útoky proti informačním technologiím, jsou popsány a také vysvětleny jejich funkce. Ze zjištěných informací vyplývá, že ne každý hacker je nebezpečný zločinec a ne každý útočník musí být nutně hacker. Motivace těchto počítačových nadšenců se různí a sami se dělí do skupin, jejichž rozdíly jsou v práci popsány. Významným společným činitelem, který hackery a jiné počítačové nadšence spojuje, je ideál svobody kyberprostoru. Na ten však naráží snaha legislativně sjednotit vymáhání práva v kyberprostoru. Jedná se o rozvíjející se právní odvětví, které má snahu o sjednocení mezinárodního boje proti kyberkriminalitě.

Průřez historií kyberterorismu nám poodhaluje pozadí několika mezinárodních konfliktů s přesahem do kyberprostoru. A dále případy použití vyspělých komplexních malwarů Stuxnet a Flame. Žádný z těchto kybernetických útoků, ale není přisuzován teroristické organizaci. Ani v současné době není pravděpodobné spáchání závažného kybeteroristického útoku ze strany některé z teroristických organizací. V širším pojmu kyberterorismu, tedy dnes zůstává hlavním nebezpečím hacktivismus a kybernetická válka.

Výsledky dotazníkového šetření poukazují na obavy veřejnosti z kyberteroristických útoků, ale zároveň neochotu zbavit se svobody kyberprostoru, za výhodu větší bezpečnosti. Pozitivním zjištěním výzkumu je vysoké procento chráněných osobních počítačů. Riziková zůstává slabší ochrana mobilních zařízení, která se můžou stát potenciální hrozbou.

Na základě zjištěných informací lze předpokládat, že provázanost reálného světa a kyberprostoru se bude i v nadcházejících letech prohlubovat, stejně jako tomu bylo doposud. S tím pravděpodobně bude souviset vzrůstající počet útoků a jejich dopady. V budoucnu nelze vyloučit, že k výčtu kyberteroristických útoků přibude některý, který půjde na vrub teroristické skupiny.

Seznam použitých zdrojů

Literární zdroje

1. DOSEDĚL, T., Počítačová bezpečnost a ochrana dat, 1. Vydání, Brno: Computer press, 2004. 182 s. ISBN 978-80-2510-106-3
2. DUNNIGAN, J., Bojiště zítřka: tváří v tvář hrozbě kybernetického terorismu, 1. Vydání, Praha: Baronet, 2004. 356 s. ISBN 80-7214-642-4
3. GLENNY, M., Temný trh, Kyberzloději, kyberpolicisté a vy, 1. Vydání, Praha: Dokořán, 2013. 272 s. ISBN 978-80-7363-522-0
4. HROMADA, M., Kybernetická bezpečnost, 1. Vydání, Praha: Powerprint, 2015. 250 s. ISBN 978-80-87994-72-6
5. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti, 3. doplněné a upravené vydání. Praha: Policejní akademie České republiky v Praze, 2015. 240 s. ISBN 978-80-7251-436-6
6. JIROVSKÝ, V., Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. Vydání, Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2
7. KOLOUCH, J., Cybercrime, 1. Vydání, Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8
8. KOLOUCH, J., VOLEVECKÝ, P., Trestněprávní ochrana před kybernetickou kriminalitou. 1. Vydání, Praha: Policejní akademie, 2013. ISBN 978-80-7251-402-1
9. MATĚJKA, M., Počítačová kriminalita. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2
10. PETROWSKI, T., Bezpečí na internetu pro všechny. 1. Vydání, Liberec: Dialog, 2014. 244 s. ISBN 978-80-7424-066-9
11. PIKNA, B., Mezinárodní terorismus a bezpečnost Evropské unie. Praha: Linde, 2006, 407 s. ISBN 80-7201-615-6
12. POŽÁR, J., Informační bezpečnost. Praha: Aleš Čeněk, 2005. 309 s. ISBN 978-80-8689-838-4
13. PROCHÁZKA, D., První kroky s internetem, 3. Vydání, Praha: Grada Publishing, 2010, 108 s. ISBN 80-2473-255-6

Elektronické zdroje

14. BITTO, O. Stuxnet: virová předzvěst třetí světové?. In: *Živě* [online]. 2010 [cit. 2017–06-05]. Dostupné z WWW: <http://www.zive.cz/clanky/stuxnet-virova-predzvest-treti-svetove/sc-3-a-153951/default.aspx>
15. DOLEJŠÍ, K. 1986 Hackerův manifest. In: *Britské listy* [online]. 2003 [cit. 2017–06-04]. Dostupné z WWW: <http://blisty.cz/art/14662.html>
16. DRMOLA, J. Konceptualizace kyberterorismu, In *Vojenské rozhledy* [online]. 2013 [cit. 2017–06-04]. Dostupné z WWW: <http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu>
17. ERBEN, L. Příchod hackerů. In: *Root* [online]. 2014 [cit. 2017–06-04]. Dostupné z: <http://www.root.cz/clanky/prichod-hackeru-zrod-kyberneticke-valky/>
18. FLÍDR, T. Mezinárodní právo kyberprostoru. In: *Kyberbezpečnost* [online]. 2008 [cit. 2017–06-08]. Dostupné z: <https://www.kyberbezpecnost.cz/?p=198>
19. GŘIVNA, T. Úmluva o kybernetické kriminalitě. In: *European* [online]. 2008 [cit. 2017–06-08]. Dostupné z: <http://www.europen.cz/Proceedings/32/Umluva%20o%20kyberneticke%20kriminalite.pdf>
20. KUŽEL, S. Kybernetická kriminalita od hackerů ke kybernetickým válkám. In *Business It*. [online]. 2012 [cit. 2017–04-30]. Dostupné z WWW: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php>
21. MINISTERSTVO VNITRA, Základní definice, vztahující se k tématu kybernetické bezpečnosti. In: *Ministerstvo vnitra* [online]. 2009 [cit. 2017–06-04]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>
22. NUTIL, P. Darknet, aneb cesta do hlubin internetu .In *Kurzy* [online]. 2015 [cit. 2017–05-04]. Dostupné z WWW: <http://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu>
23. Pojmy – terorismus, In *mvcr.cz* [online]. 2017 [cit. 2017–05-30]. Dostupné z WWW: <http://www.mvcr.cz/clanek/pojmy-terorismus.aspx>
24. Pojmy – Kybernetický terorismus – kyberterorismus, *mvcr.cz* [online]. 2017 [cit. 2017–05-30]. Dostupné z WWW: <http://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx>

25. PAVLÍKOVÁ, M. Estonsko – Ruský incident v kontextu kyberterorismu, In *Global Politics* [online]. 2014 [cit. 2017–06-04]. Dostupné z WWW: <http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu>
26. SEKERA, T. Kybernetické útoky: Rusko? – Gruzie a svět. In *mvcr.cz* [online]. 2008 [cit. 2017–06-05]. Dostupné z WWW: <www.mvcr.cz/soubor/zpravodajstvi-dokumenty-prezentace-spolecnosti-logica.aspx>
27. TOMEŠ, M. Průmysl prochází změnou jako nikdy předtím, říká autor knihy o internetu věcí. In *E15* [online]. 2017 [cit. 2017–06-04]. Dostupné z WWW: <http://e-svet.e15.cz/it-byznys/prumysl-prochazi-zmenou-jako-nikdy-predtim-rika-autor-knihy-o-internetu-veci-1333263>
28. WEISS, G. W., 2008. The Farewell Dossier, In: *Central Inteligence Agency* [online] 2008 [cit. 2017–06-04]. Dostupné z WWW: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm>
29. WEISS, J. Maroochy Water Services Case Study. In *Computer security division, Computer security reource center* [online]. 2008 [cit. 2017–06-04]. Dostupné z: <http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf>

Legislativní dokumenty

1. ČESKO. Zákon č. 2/1993 Sb., Listina základních práv a svobod: In *Sbírka zákonů, Česká republika*. 1992, částka 1, s. 19 - 20. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426>. ISSN 1211-1244.
2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 394 - 426. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>. ISSN 1211-1244
3. ČESKO. Zákon č. 89/2012 Sb., občanský zákoník: In *Sbírka zákonů, Česká republika*. 1993, částka 33, s. 1026 - 1027. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=24084>. ISSN 1211-1244

4. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In *Sbírka zákonů, Česká republika*. 2014, částka 75, s. 1928. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231>. ISSN 1211-1244

Seznam zkratek

CERT – Computer Emergency Response Team, skupina pro reakce na počítačové, bezpečnostní incidenty

CIA – Central Intelligence Agency, ústřední zpravodajská služba USA

DDoS – Distirbuted Denial of Service, typ útoku proti informačním technologiím zahlcením webové služby

DNS – Domain Name Systém, systém doménových jmen

ETA – Euskadi Ta Askatasuna, Baskická teroristická organizace

FBI – Federal Bureau of Investigation, Federální úřad pro vyšetřování

GPS – Global Positioning Systém, globální polohový systém

ICQ – I Seek You, software pro komunikaci

IP – IP adresa je číselný kód identifikující síťové rozhraní

IRA – Irská republikánská armáda

SCADA - Supervisory Control And Data Acquisition, jedná se o centrální systémy určené k řízení a sběru dat

TNT – Trinitrotoluen, jedná se o trhavinu

USB – Universal Seriál Bus, je univerzální sériová sběrnice, která se používá k propojení počítače a periferních zařízení

WWW – World Wide Web, celosvětová počítačová síť

Seznam tabulek a grafů

Graf 1: Vyhodnocení otázky č. 1 - Pohlaví

Graf 2: Vyhodnocení otázky č. 2 – Věk

Graf 3: Vyhodnocení otázky č. 3 - Vzdělání

Graf 4: Vyhodnocení otázky č. 4 - Myslíte, že je kyberterorismus aktuální problém?

Graf 5: Vyhodnocení otázky č. 5 - Myslíte, že je kyberterorismem ohrožena Česká republika?

Graf 6: Vyhodnocení otázky č. 6 - Myslíte, že je Česká republika připravena čelit kybernetickým hrozbám?

Graf 7: Vyhodnocení otázky č. 7 - Máte obavy z kybernetických hrozeb?

Graf 8: Vyhodnocení otázky č. 8 - Souhlasíte, se sledováním Vašich internetových aktivit, pod záminkou zvýšení bezpečnosti?

Graf 9: Vyhodnocení otázky č. 9 - Chráníte svůj počítač pomocí antivirového programu?

Graf 10: Vyhodnocení otázky č. 10 - Provádíte aktualizace, když Vás systém upozorní?

Graf 11: Vyhodnocení otázky č. 11 - Máte mobilní zařízení s připojením na internet?

Graf 12: Vyhodnocení otázky č. 12 - Chráníte své mobilní zařízení antivirovým programem?

Přílohy

Příloha č. 1 – Dotazník

1. Pohlaví:

- [ ] Muž
- [ ] Žena

2. Věk:

- [ ] 14 - 25 let
- [ ] 26 - 35 let
- [ ] 36 - 59 let
- [ ] 60 let a více

3. Vzdělání:

- [ ] Střední
- [ ] Vysokoškolské
- [ ] Vyšší odborné
- [ ] Základní

4. Myslíte, že je kyberterorismus aktuální problém?

- [ ] Ano
- [ ] Ne

5. Myslíte, že je kyberterorismem ohrožena Česká republika?

- [ ] Ano
- [ ] Ne

6. Myslíte, že je Česká republika připravena čelit kybernetickým hrozbám?

- [ ] Ano
- [ ] Ne

7. Máte obavy z kybernetických hrozeb?

- [ ] Ano
- [ ] Ne

8. Souhlasíte, se sledováním Vašich internetových aktivit, pod záminkou zvýšení bezpečnosti?

- [ ] Ano
- [ ] Ne

9. Chráníte svůj počítač pomocí antivirového programu?

- [ ] Ano
- [ ] Ne

10. Provádíte aktualizace, když Vás systém upozorní?

- [ ] Ano
- [ ] Ne

11. Máte mobilní zařízení, s připojením na internet?

- [ ] Ano
- [ ] Ne

12. Chráníte své mobilní zařízení antivirovým programem?

- [ ] Ano
- [ ] Ne