VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH

STUDIÍ, Z.Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÝ TERORISMUS

Autor práce: Ladislav Teml

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Josef Kříha

Katedra: Právních oborů a bezpečnostních studií

2019

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

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

…….

Děkuji vedoucímu bakalářské práce Mgr. Bc. Josefu Kříhovi za cenné rady, trpělivost, připomínky a metodické vedení práce. Dále bych chtěl poděkovat mé rodině, především mé manželce Márii Temlové, za trpělivost a shovívavost během zpracování této práce.

ABSTRAKT

TEML, L. *Kybernetický terorismus: Bakalářská práce*, České Budějovice: Vysoká škola evropských a regionálních studií, o.p.s., 2019. 62 s. Vedoucí práce: Mgr. Bc. Josef Kříha.

Klíčová slova: kyberterorismus, kybernetický útok, kyberprostor, kybernetické zbraně, legislativa.

Bakalářská práce se zabývá problematikou kybernetického terorismu. První část práce popisuje vývoj a historii terorismu a definuje terorismus jako pojem. Definuje také kybernetický prostor a zabývá se nástroji pro kybernetický útok. Další část práce pojednává blíže o kybernetickém terorismu, jeho aktérech a nástrojích kybernetického terorismu. Třetí a čtvrtá část této práce pojednává o legislativní úpravě norem v České republice a mezinárodních normách v oblasti kybernetické kriminality a kybernetického terorismu. Závěrečná část práce je věnována analýze vybraných kybernetických útoků a jejich vyhodnocení.

ABSTRACT

TEML, L.: *Cyber Terrorism: Bachelor thesis*. České Budějovice: The College of European and Regional Studies, 2019, 62 p. Supervisor: Mgr. Bc. Josef Kříha

Key words: cyberterrorism, cyber attack, cyber space, cyber weapons, legislation.

The bachelor's thesis deals with the issue of cyber-terrorism. The first part of the thesis describes development and history of terrorism and defines the term terrorism. This part also defines the term cyber space and deal with tools for cyber attacks. The next part is about cyberterrorism, cyberterrorists and cyberterroristic tools. The third and fourth part of the thesis deal with the legislative regulation of standards in the Czech Republic and international standards in the field of cybercrime and cyber terrorism. The final part is devoted to the analysis of selected cyber attacks and their evaluation.

OBSAH

ÚVOD

V historii lidstva terorismus není ničím novým a nejedno období je provázeno krvavými převraty, útoky na civilní obyvatelstvo a teroristickou absolutní vládou. A ačkoliv v posledních letech jsou slova terorismus, terorista a teroristický útok užívány, skloňovány, v některých případech i zneužity a překrouceny politiky, medii a veřejností, nejsou zpravidla užity v odborném pojetí významu, ale v populistické rovině a překrucují samotný význam těchto slov. V současné době je také aktuální otázka jedné specifické formy teroristického útoku, kterou je útok na nebo za pomoci moderních informačních technologií. Bližší specifikací je útok na počítače, počítačové sítě a inteligentní systémy, kdy jejich vyřazení či poškození je strategickým cílem, neboť v současné době žijeme v informační společnosti[1] a tyto moderní technologie se pro naši společnost staly životně důležité a stále více se stávají páteřním systémem naší společnosti, proto je tedy část útoku vedena proti těmto technologiím nebo jejich prostřednictvím. Tento způsob teroristického útoku je nazýván kyberterorismus. Jak bude dále uvedeno z definice terorismu, teroristického činu a kybernetického terorismu, né každé konání a útok je teroristickým nebo kyberteroristickým činem, ale jedná se pouze o kybernetický útok nebo kybernetický zločin.

V moderní a technicky vyspělé společnosti je tedy ochrana dat a technologií v kyberprostoru naprostá nezbytnost. Neboť rozsáhlé kybernetické útoky znamenají nejenom možnou paralýzu, ale ohrožení lidských životů v případě poškození nebo vyřazení strategických zařízení, kterými jsou objekty výroby a distribuce energetiky, objekty dopravní infrastruktury, objekty finančních institucí, veřejné správy a telekomunikační síť. Navíc v současné době aktuálního tématu internetu věcí je možné cíleným útokem zasáhnout nejenom veřejné objekty, ale jedním úspěšným útokem je teoreticky možné zasáhnout velké množství domácností s využitím internetu věcí a paralyzovat nebo ovládat jejich vnitřní zařízení. Proto je nutné a nezbytné, pracovat na zabezpečení a ochraně dat na všech úrovních moderní společnosti a to mezinárodní, národní, korporátní i personální a aplikovat ji nejenom v technickém, politickém a legislativním pojetí. V rámci moderní společnosti by ochrana dat a kyberprostoru měla

[1] JANOUŠEK, Michal, Kyberterorismus: Terorismus informační společnosti, In Obrana a strategie [online]. 20.03.2007, [cit. 2019-05-10]. Dostupné z WWW: <https://www.obranaastrategie.cz/filemanager/files/6513.pdf>

být promítnuta nejen do legislativní a technické ochrany, ale současně i do vzdělávacího systému nebo aplikována jako všeobecná znalost, čímž by fakticky vzrostla obranyschopnost od jedince po velké spolky.

1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem práce je za pomoci komparace a analýzy odborné literatury, odborných článků a dalších relevantních zdrojů zhodnotit a definovat kybernetický terorismus. A to především objasnit základní pojmosloví a východiska zkoumané oblasti, kterými jsou například terorismus, kybernetický prostor, kybernetický útok. Práce se v rámci samostatných subkapitol zaměřuje na monitoring, zpracování a vyhodnocení odborných informací o samotném kyberterorismu a to způsobem analýzy a definice elementárních pojmů jako kybernetický útok, kdo je aktérem kybernetického terorismu, jaké jsou jeho cíle a jak je využit kyberprostor v rámci útoků.

Vedlejším cílem práce je analyzovat a zhodnotit možná protiopatření před kybernetickými útoky a to jak v legislativní rovině, tak politické a i v rámci preventivních bezpečnostních opatřeních při boji proti kybernetickému terorismu u nás i v zahraničí. A následně predikovat možné směřování kybernetických teroristických útoků.

Empirická část práce se věnuje v rámci kazuistiky vybraným útokům vedených v kyberprostoru a na základě analýzy jejich způsobu provedení, cílů a následků, bude provedeno zhodnocení, zda se v daném případě jedná o kybernetický teroristický čin nebo jen pouze o kybernetický zločin. V intencích empirické časti práce bude formou dílčích a zevšeobecňujících závěrů demonstrováno možné směřování kybernetického terorismu v budoucnosti.

Během zpracování práce byly formou analýzy, rešerše a komparace využity aktuální poznatky zkoumané oblasti z dostupné odborné literatury, pramenů či internetových zdrojů, včetně účinné mezinárodní i vnitrostátní právní úpravy vztahující se ke zkoumané problematice.

Věcná část práce je rozdělena do pěti subkapitol. V první kapitole je uvedena metodika a cíle práce. Druhá kapitola se věnuje vymezení základních pojmů, kterými jsou terorismus, kyberprostor, kybernetický útok a kybernetický terorismus samotný. Třetí a čtvrtá kapitola se věnuje legislativní ochraně před kybernetickými útoky v České republice a na mezinárodní úrovni. Pátá kapitola je empirickou částí práce, kdy za předem daných hodnotících elementů jsou komparovány s těmito jednotlivé případové studie s výslednou analýzou a vyhodnocením jednotlivých případových studií.

2 DEFINICE KYBERNETICKÉHO TERORISMU

2.1 Vymezení základního pojmosloví

2.1.1 Terorismus

Jev, který označujeme jako kybernetický terorismus, je jevem moderním a přichází teprve s nástupem moderních komunikačních médií. Tento jev je však speciálním jevem k známému terorismu, jehož vývoj se datuje od počátku lidského společenství. Pojem terorismus se formuje a definuje v rámci dějin vždy podle náhledu společnosti a jeho vnímání společenských událostí, a proto pojem terorismus je těžké vymezit. Samotné slovo terorismus vychází z pojmu teror, který je odvozen z latinského slova terrere, jehož překlad je vykládán jako strašný či hrozný.[2] Pokud provedeme historický exkurz, zjistíme, že už v dobách rozmachu římské říše je jistá forma terorismu páchaném Římany, jde o takzvanou ničivou válku nebo trestnou válku, kdy jsou mimo vojenských cílů ničeny i celé vesnice a obyvatelé povražděny. Toto jednání má psychologický efekt na nepřítele, kdy ztrácí odvahu k dalšímu boji nebo přestává podporovat protiřímský odpor. Dalším milníkem jsou křižácké války a sekta Hassasinu (nebo také Assasini), kteří prováděli plánované úkladné vraždy, vždy veřejně a velmi brutálním způsobem. Jejich odpůrci (Saladin, Templáři a další) téměř ztratili vůli k boji s touto sektou a jejich ideály, neboť nebezpečí, které znamenal boj s Hassasiny bylo příliš vysoké a nikdo z vysokých hodnostářů se nechtěl stát cílem těchto vrahů. Z historického pohledu by se dalo říci, že tato sekta je předchůdcem moderních radikálních islámských teroristických organizací. Dalším výrazným milníkem v historii terorismu je počátek 18. století. V tomto období je kolonizována Severní Amerika a boj s indiány o území se z konvenční války a bojů zvrhává k masakrování všech nepřátel, často po vítězství jedné strany dojde k totálnímu masakru zbylých vojsk a dalšího civilního obyvatelstva. Evropa pozvolna přechází v etapu nacionalistickou, kdy se v mnohonárodnostních společenstvích v některých skupinách objevuje a vzrůstá nacionalistické cítění a s tím touha po osamostatnění národa nebo území, kdy pozorujeme útoky jak proti státní moci, tak i silné represivní opatření ze strany mocností proti revolucím a vzpourám. Dále je zde jistá skupina útočníků, kteří jsou také nazýváni „anarchisté“ a ti při svých útocích využívají

[2] BRZYBOHATÝ, Marian. *Terorismus I*. Praha: Police History, 1999. ISBN 80-9026-70-1-7. s. 11-20

nejenom vraždy, ale také bombové útoky a jiné násilí, aby na sebe upozornili a bojovali proti nerovnostem ve společnosti a kladli si za cíl svrhnout vlády, a moc předat do rukou dělníkům. Konec období průmyslové revoluce a nástup dvou světových válek s sebou přináší nové formy násilí, krutostí a teroru, kdy je zaveden pojem „totální válka“, který s sebou nese nové pojetí konvenční války, kdy se mimo vojenských cílů útočí také na civilní cíle a obyvatelstvo. Ale právě v průběhu druhé světové války je užito cílevědomé vedení války proti civilnímu obyvatelstvu tak, že bylo využito vojenské síly a vyhlazování civilního obyvatelstva na dobytém území a aktérem největšího teroru v této době se stal německý vůdce Adolf Hitler, kdy však ani na straně spojenců nebyla šetrnost k civilním cílům během války velká, což ostatně dokazuje útok na Hirošimu a Nagasaki. Po druhé světové válce se po rozdělení sfér vlivu mezi západem zastoupeném USA a východem zastoupeném Sovětským svazem svět ocitl v takzvané „Studené válce“, jež představovala závody ve zbrojení a upevňování svého vlivu a snižování vlivu opačného. V tomto období vznikali už pravidelné teroristické skupiny, financované a podporované státními subjekty. Jejich způsob boje se vyznačoval prvky vojenské taktiky, využití vojenských konvenčních zbraní a prostředků na útoky proti civilním cílům, jež tvořili především politici, diplomaté, velké průmyslové firmy a později také i letadla, sportoviště, vlaky, letiště a nádraží. Ke každému útoku se vždy přihlásila nějaká teroristická skupina. V této době byl terorista brán jako odvážný odbojář bojující proti cizí mocnosti a snažící se osvobodit se ze sféry vlivu této mocnosti. Většina aktérů se v této době hrdě hlásila ke své skupině. Řada teroristických skupin počala také operovat mimo země, kde vznikaly a dostaly se tak na mezinárodní úroveň. Na počátku 80. let se objevuje fenomén sebevražedných útoků, kdy se útočníci při útoku obětují, aby dosáhli co možná největšího hromadného účinku, typicky auto naložené náloží nebo trhavinový pás kolem těla. Konec studené války s sebou přinesl mnoho změn a to i v motivaci mezi teroristy, jak uvádí M. Brzybohatý[3], dochází k transformaci ideologického pojetí terorismu na pohnutky nacionalistické a náboženské. Teroristické skupiny rozšiřují své členské základny a operativní prostor, expandují do dalších států, kde zakládají buňky, tím se stávají globální hrozbou. Mimo náboženského a nacionalistického teroru, díky rozpadu sovětského svazu a možným chybám při likvidaci zbraní v rámci

[3] BRZYBOHATÝ, M. Současný terorismus. Vojenské rozhledy. Praha, 2002, roč. 11 (43), č. 2, s. 46—62. ISSN 1210-3292.

odzbrojování státu vyvstává otázka nebo hrozba ZHN terorismu neboli tzv. „superterorismu“. Další forma terorismu, který v současné době vzniká a váže se k vývoji nových technologií, k zavedení a masovému rozšíření internetu je tzv. kybernetický terorismus, neboli také kyberterorismus.

Pokud budeme definovat kybernetický terorismus jako jednu z forem terorismu, která ke svému spáchání využívá nástroje kyberprostoru a jeho účinky se promítají buď v elektronickém světě, ale také ve světě reálném, musíme definovat terorismus jako takový. Všeobecně by se pojem terorismus dal definovat jako užití síly k dosažení stanoveného cíle, což vystihuje i konvenční válku a guerillu. Proto můžeme terorismus obecně řadit mezi způsoby vedení boje, ke kterým patří výše zmíněné vedení konvenční války a guerillový způsob boje neboli guerilla. Co však terorismus od ostatních způsobů boje odlišuje je motivace, cíle a způsob vedení útoku (v mnohém je však podobný guerille i konvenčnímu válčení). Přesná definice terorismu tedy vyplývá z vymezení jeho formy, způsobu provedení a cílů a je to tedy způsob boje vedený především v utajení, kdy snahou útočníků je zasáhnout strategické civilní cíle nebo zajistit, co nejvyšší početní ztráty na civilním obyvatelstvu a tím způsobit největší možný rozkladný psychologický účinek na nepříteli, který by oslabil jeho vůli a následně jednal podle požadavku útočníka.

V knize Vybrané aspekty terorismu[4] autoři definují charakteristické znaky vymezující terorismus a to následovně:

- předem promyšlená a plánovaná akce;
- útočník své konání chápe jako poslání k splnění stanoveného cíle;
- útočníci infiltrují cílové prostředí a působí v utajení;
- nezákonné užití nebo hrozba užití různých forem násilí se značným psychologickým dopadem;
- cílem jsou především civilní cíle a civilní obyvatelstvo;
- primární cíl útoku je vyslat vážné zastrašující poselství;

[4] ŘEHÁK, David, Pavel FOLTIN a Richard STOJAR. Vybrané aspekty soudobého terorismu. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2008. ISBN 978-80-7278-443-1. s 8

- útoky jsou realizovány především nestátními skupinami nebo organizacemi.

Marian Brzybohatý ve své knize Terorismus I. uvádí definici terorismu podle americké ústavy a to následovně:

„V roce 1980 byla v USA publikována definice terorismu, jež se stala výchozím standardem pro posuzování a hodnocení teroristických činů. Zní takto: „Terorismus je propočítané použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen.‘“[5]

Český právní řád a zejména trestní zákoník[6] definuje teroristický útok v § 311 a teror v § 312, kdy ve skutkové podstatě tohoto činu definici terorismu rozšiřuje a také formálně vymezuje jednání, které je teroristickým činem v rámci právního zřízení České republiky (pozn. autora: skutková podstata uvedených trestných činů je v práci umístěna v kapitole 3.2).

2.1.2 Kyberprostor

Samotný pojem kyberprostor vychází z anglického slova cyberspace. Toto slovo užil a definoval poprvé v 80. letech spisovatel William Gibson:

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se u čí základy matematiky. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla se řazené v ne-prostoru mysli, shluky a souhvězdí dat.“[7]

---

[5] BRZYBOHATÝ, Marian. *Terorismus I*. Praha: Police History, 1999. ISBN 80-9026-70-1-7. s. 11

[6] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 394 - 406. Dostupné z WWW:< https://www.zakonyprolidi.cz/cs/2009-40 >

[7] KUŽEL, S. Kybernetická kriminalita od hackerů ke kybernetickým válkám. In Business It. [online]. [cit. 2019–04-30]. Dostupné z WWW: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php>

Vzhledem k rozvíjející se kultuře informačních technologií se termín kyberprostor velice rychle ujal a vžil se do podvědomí. William Gibson později své pojetí kyberprostoru sám kritizoval a v interview z roku 1995 kyberprostor definoval následně:

„Kyberprostor je metafora, které nám umožňuje uchopit toto místo, kde se od druhé světové války vytvořilo a vytváří stále více a více věcí, které dnes chápeme jako součást naší kultury. Kyberprostor je tam, kde obchodujeme, místo kde mají banky uložené své a naše peníze, stejně tak zde probíhají burzovní obchody. Je to pro všechny zúčastněné praktické, protože se jedná o pouhý pohyb dat.“[8]

Současné a zatím jedno z nejlépe vystihujících pojetí kyberprostoru uveřejnil Marco Mayer se spoluautory:

„Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace.

Kyberprostor zahrnuje:

a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, chytré telefony/tablety, počítače, servery, atd..),

b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému,

c) spojení počítačových sítí,

d) síť sítí spojujícími počítačové systémy (oproti spojení počítačových sítí je rozdíl jen v organizaci sítí),

d) uživatelské vstupy a uzly zprostředkovatelů spojení,

[8] "I DON'T EVEN HAVE A MODEM", interview Jan Josefsson, 1995. [online]. [cit. 2019–04-30], dostupné na: http://www.josefsson.net/gibson/index.html

e) informace – uživatelská data.“[9]

Výše zmíněné poznatky je možné shrnout v legálním pojetí samotného kyberprostoru podle § 2 písm. a) ZKB, který uvádí, že *„kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*[10]

V obsahovém pojetí je možné si samotný kyberprostor představit jako ledovec, kdy pomyslným kouskem nad hladinou je běžnému uživateli volně přístupný prostor v rámci ICT. Tato část je nazývána „Surface web“ a zaujímá přibližně 4 % podílu v celkovém kyberprostoru. Další část pod hladinou navazující na surface web je tzv. „deep web“. Tato část zaujímá největší rozlohu v kyberprostoru, kdy se jedná o 90% všech dat na internetu. Běžný uživatel se do prostoru deep webu nedostane bez užití speciálních ICT nástrojů a znalostí. Na pomyslném opačném vrcholu surface webu existuje tzv. „dark web“. Dark web funguje na stejném principu jako deep web, avšak informace zde sdílejí různé zájmové skupiny a zločinci. Jedná se o sofistikovaný systém umožňující anonymní sdílení dat, anonymní obchody s nelegálními předměty či daty, nástroje k legalizaci výnosů trestné činnosti a také možné vybavení pro teroristy, neboť se zde dají získat prostředky pro konvenční i kybernetický útok.[11]

---

[9] Definition by Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, Draft Pisa . [online]. [cit. 2019–04-01], dostupné na WWW: <https://www.academia.edu/7096442/How_would_you_define_Cyberspace>

[10] ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2014-181#redakce>.

[11] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. str. 46-53

Obrázek č. 1 Složení cyberpsace[12]

2.1.3 Kybernetický útok

Jirásek a kol. definují kyberneticky útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“*[13]

Takto uvedená definice v sobě zahrnuje dva aspekty útoku a to poškození počítačového systému a zároveň i získání dat či informací. Ale reálně se během kybernetického útoku můžeme setkat pouze s formou zahrnující jenom poškození nebo vyřazení počítačového systému, a nebo s formou zahrnující pouze extrakci dat. Jako příklad mohou sloužit útoky DoS, které jsou vedeny pouze za účelem

[12] Zdroj: Quora, 22.06.2018 [online]. [staženo 2019–04-01], dostupné na WWW: <https://www.quora.com/Does-the-Deep-Web-Dark-Web-and-Marina-Web-really-exist>

13 JIRASEK, Petr, Luděk NOVAK a Josef POŽAR. Výkladový slovník kybernetické bezpečnosti. [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 59. Dostupný na WWW: <http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/>

potlačení distribuované služby, jejich cílem tedy není poškodit počítačový systém samotný, jakkoliv si zajistit do tohoto systému přístup a ani extrahovat data. Kybernetický útok může být definován jako „jakékoliv protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby.“[14] Tato definice v sobě nezahrnuje některé činy, zejména ty, které nelze kategorizovat jako protiprávní a jsou pouze nemorální či nechtěné.

Jenda z možných definic kybernetického útoku je obsažena v ZKB, i když jsou zde užity jiné pojmy a není zde přímá definice kybernetického útoku. ZKB definuje v § 7 kybernetickou bezpečností hrozbu a kybernetický bezpečnostní incident následovně:

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.“*[15]

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.“*[16]

2.1.4 Nástroje kybernetických útoků

Současný trend vývoje ICT dává velké množství možností využití připravených nástrojů ke kybernetickému útoku, některé jsou volně šířeny a některé jsou poskytnuty za úplatu. Moderní vysokoúrovňové programovací jazyky (příkladem je jazyk Python nebo Java) jsou intuitivní a lehce osvojitelné, na rozdíl od nízko úrovňových jazyků (typickým příkladem je jazyk C). Některé vysokoúrovňové jazyky svým principem znemožňují nebo stěžují jejich užití k poškození dat nebo informací na uživatelských

[14] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. s. 55

[15] ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2014-181#redakce>. § 7 odst. 1

[16] ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2014-181#redakce>. § 7 odst. 2

stanicích, jiné jazyky tyto principy nemají ve svém zdrojovém kódu obsaženy a jsou vhodné pro vývoj útočných programů. Příkladem takového jazyka je třeba Python, má intuitivní a lehce osvojitelnou syntaxi, je multiplatformní a má velkou podporu knihoven, což ho určuje už předem jako dobrý nástroj pro vývoj různých programů a utilit, které nemusí být vždy ku prospěchu uživatele. Tyto sofistikované nástroje tak umožňují vést kybernetický útok i útočníkům, kteří nejsou ICT experty. Kvalita a účinnost těchto nástrojů ve většině případů nemusí být na takové úrovni, aby znamenala bezpečnostní hrozbu, ale v případě správného a úspěšného užití mohou znamenat nemalé finanční ztráty, ochromení kritické infrastruktury nebo i ztráty na životech.

2.2 Kybernetický terorismus

Kybernetický terorismus je jednou z největších globálních hrozeb moderního světa. Jeho principem je zneužití informačních technologií jako prostředku a prostředí k útoku na data či infrastrukturu umožňující vést útok na cíl z neomezeně vzdáleného místa. Útoky jsou vedeny z pravidla malými vojensky neorganizovanými skupinami, kdy jejich motivace je náboženského nebo polického charakteru. Útok samotný je jen prostředkem k dosažení cíle, je vždy směřován k vyvolání nátlaku na změnu postoje, názoru, veřejného mínění či donucení k jednání, prostřednictvím strachu a pocitu ohrožení. Kybernetický terorismus je zpravidla klasifikován jako neletální forma terorismu. Rozvoj informačních technologií a zejména internetu věcí však umožňují případným útočníkům za pomoci kybernetického útoku způsobit následky také v reálném světě.

2.2.1 Aktéři kyberterorismu

Rozdělení samotných aktérů kyberterorismu můžeme dělit podle různých faktorů, jedním z nich je geopolitické členění:

Teroristé

V současné době nejsou známy údaje, které by potvrzovali nebo vyvraceli existenci ICT odborníků jako členů mezinárodních teroristických skupin, vývoje kybernetických zbraní a ani není známá úroveň znalostí a rozsah jejich dovedností v této oblasti. Užití nástrojů kybernetického terorismu je pro tyto organizace spíše

podpůrnou činností, kdy hlavní útoky jsou vedeny konvenčně a kyberprostor je užit spíše pro získání informací, získání financí, nábor rekrutů, komunikaci, plánování, koordinaci a propagaci myšlenkových idejí skupiny a jejich činů prostřednictvím webu a sociálních médií, neboť tak mají největší efekt a dopad. Kybernetické útoky jsou tedy jen doprovodným jevem útoku v reálném světě. Konvenční útoky jsou pro teroristické organizace v současné době mnohem výhodnější, levnější a efektivnější než kybernetický útok. Nesmíme však opomenout jeden fakt, kdy k posledním teroristickým útokům v Evropě byla užita vozidla, která byla řízena samotnými teroristy. Nebezpečí kybernetického útoků v této oblasti vzniká ve vývoji a provozu autonomních ovládacích systému vozidel a možnosti převzetí jejich ovládání teroristy prostřednictvím kybernetických nástrojů a následné využití těchto prostředků vůči měkkým cílům.[17,18]

Nepřátelské národní státy

V současné době je největší hrozbou kybernetický útok vedený profesionálními hackery financovanými nepřátelským státním sektorem, neboť mnoho států v současné době vyvíjí vlastní nástroje a prostředky kybernetických útoků a obrany. Prozatím jsou tyto nástroje užity jen pro dezinformační válku a špionážní aktivity v oblasti vojenství, průmyslu a financí. Kybernetické nástroje jsou velmi oblíbené v současném pojetí vedení asymetrické války, neboť umožňují způsobit ekonomické i informační ztráty nepříteli, který nad vámi má převahu v reálném světě. Největšími potencionálními útočníky pro státy NATO, potažmo USA je Kuba, Čína, Rusko a Severní Korea, které mimo jiné pracují i na vývoji vlastních kybernetických zbraní.[19]

Na základě konfliktů mezi Čínou a USA je jasné, že obě země disponují silnou základnou hackerů, nikdy se však nepotvrdilo, že jsou ve službách daných vlád. A

[17] BRUNE, Štěpán, Hacker může útočit i pomocí chytré televize, říká výzkumník počítačových virů Jiří Gogela, e15.cz [online], 27.03.2019 [citace 2019–04-10], dostupné na WWW: <https://www.e15.cz/rozhovory/hacker-muze-utocit-i-pomoci-chytre-televize-rika-vyzkumnik-pocitacovych-viru-jiri-gogela-1357483>

[18] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 132-133

[19] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 133

samotná Čína odmítá jakoukoliv zodpovědnost za útoky vedené hackery z jejího území.

Sympatizanti teroristů a protiameričtí hackeři

Z historických trendů vychází, že kybernetické útoky na státní zřízení USA nebo dalších spojenců páchají spíše sympatizanti teroristických hnutí a protiamericky nebo protiglobalisticky smýšlející jedinci či organizace, nežli teroristé samotní. V případě, kdy USA bude svoji protiteroristickou politiku vést také proti islámu, je možné, že se do konfliktu zapojí i promuslimské hackerské skupiny (G-Force, The Pakistan Hackerz Club, Doctor Nuke a jiné). V těchto konfliktech hrají velkou úlohu také čínští hackeři, kteří svou podporou ostatních hackerských skupin či samotnými útoky znamenají velké bezpečností riziko na poli kybeprostoru.[20]

Čína podle oficiálních vyjádření nijak hackerské útoky nepodporuje, je však až příliš jasné, že přiznání v tomto ohledu by značilo mezinárodní konflikt, na svou obranu uvádí, že ačkoliv má a cvičí jednotku pro kybernetickou válku, je tato jednotka čistě obraným nástrojem, neboť se samotná Čína stává terčem mnohých kybernetických útoků.

Vyhledávači vzrušení (thrill seekers)

Téměř každý sledovaný kybernetický konflikt přitáhne velkou pozornost dalších hackerů, kteří si chtějí zvýšit svoji prestiž a přitáhnout na sebe pozornost, velkou skupinou těchto hackerů jsou tzv. „script kiddies“ neboli hackeři začátečníci či amatéři s nízkou úrovní znalostí. Jejich motiv pro kybernetický útok nemá politický ani náboženský podtext. Tito útočníci jsou vedeni pouze vidinou osobního prospěchu ve formě získání uznání a prestiže v komunitě hackerů. Ačkoliv je tato skupina útočníků nejpočetnější, má v roli kybernetických hrozeb nízkou váhu, protože jejich útoky ve většině případů nejsou tak sofistikované, aby vážně ohrozili západní počítačové systémy. Zůstává ale pravdou, že ačkoliv tyto útoky nejsou velkou

[20] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 133

hrozbou, mohou být náhodně úspěšné a vyřadit kritickou infrastrukturu s rozsáhlým ekonomickým dopadem.[21]

Dalším možným hlediskem pro členění aktérů kybernetických nebo spíše kyberteroristických útoků je členění podle motivace:

Hacker začátečník – jedná se o hackera s nízkou úrovní znalostí ICT a malými zkušenostmi, je přechodovým článkem mezi hackerem profesionálem a obyčejným uživatelem. Využívají ve větší míře spíše volně dostupná hotová řešení utilit a programů a díky tomu představují menší hrozbu pro moderní počítačové sítě a systémy oproti profesionálním hackerům. Jejich motivace k útoku je snaha získat prestiž v komunitě hackerů. Volba jejich cílů je čistě náhodná a útočí na vše, co mohou a co uznají za vhodné pro útok, proto jejich útok nejde typizovat a předvídat.

Hacker profesionál – typicky se jedná o znalce v oboru ICT preferující přístup a myšlenku hackerství spočívajícím ve svobodném přístupu ke zdrojům, datům a internetu. Tito jedinci neuznávají osobní vlastnictví, zákony, normy, autority ani autorská práva. Jejich útoky jsou motivovány touhou o překonání intelektuálních výzev a překážek tzv. „internetovým exhibicionismem“ a umožnění přístupu k informacím zdarma celé široké veřejnosti. Jejich nástroje jsou často distribuovány ambiciózním začátečníkům (hackerům začátečníkům), kteří místo nich provádějí samotné útoky a oni jsou jen jistou formou spolupodílníky na těchto útocích.

Virový tvůrce – jedná se o velmi specifickou skupinu odborníků ICT v oblasti programování a bezpečnosti. Jejich motivace může pocházet z osobní oblasti, kdy se jedná buď o „nedoceněné odborníky“ nebo „zrazené idealisty“ a jejich pomsta je směřována buď proti konkrétní skupině, firmě, státu nebo společnosti jako takové. Také se může jednat o překonání intelektuální výzvy v podobě vytvoření dokonale adaptabilního cíleného malwaru. Viroví tvůrci útočí v podstatě na cokoliv a jejich hlavní cíle jsou převážně počítačové systémy a sítě.

Vnitřní nepřítel – jedna z nejhorších forem útočníka. Jedná se o zaměstnance či člena organizace, který je zpravidla znalý ICT oboru a je na obdobných pozicích. Tito útočníci jsou zpravidla zhrzení zaměstnanci, kteří touží po odplatě. Nebo se také může

[21] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 134

jednat o jedince, který ve své touze po finančním prospěchu začne pracovat pro nepřátele či konkurenci či nasazeného agenta zvenčí. Při jejich útoku můžou vzniknout nemalé ekonomické škody. Jejich cílem jsou zpravidla počítačové systémy, sítě a data dané společnosti.

Informační válečník – další nebezpečný typ útočníka, který je velmi dobře znalý ICT technologií a je ochoten je využít nebo zneužít v rámci svého osobního nebo finančního prospěchu. Zpravidla se jedná o profesionála se znalostí a výcvikem v bezpečnosti ICT. Typické útoky jsou vedeny za účelem destabilizace či poškození integrity dat nebo nabourání informačních systémů na úrovni kontroly rozhodovacích procesů. K dosažení požadovaných výsledků využívá tradičních i netradičních metod, postupů a technologií, svých hlubokých znalostí v oboru bezpečnosti ICT.

Zloděj – jedná se zpravidla o osoby průměrně znalé oboru ICT, které své znalosti využívají k dosažení finančního zisku. Jejich útoky jsou zejména zaměřeny na získání přihlašovacích údajů a jejich následné využití k finančnímu obohacení. Se zkušenostmi se jejich úroveň znalostí ICT zvyšuje.

Profesní kriminálník – osoba, jejíž znalosti v oboru jsou nadprůměrné a využívá je zejména pro své obohacení. Ze svého postavení za úplatu nebo získání zisku pravidelně překračuje zákon a páchaním trestné činnosti prostřednictvím informačních technologií se živí. Jeho motivací jsou peníze a zisk. Nechává se často najímat.

Kybernetický chuligán – jedinec s odbornějšími znalosti v oblasti ICT. Jeho znalosti mu umožňují vytvářet vlastní skripty většinou v oblasti webových technologií. Jeho motivací je vlastní sláva a medializace jeho činů. Jeho útoky jsou směřovány tak, aby byly mediálně atraktivní a zviditelnili ho. Typickými útoky je defacement neboli záměna webových stránek různých státních i polostátních organizací, dále podvody, krádeže identit, peněz z účtů a platebních karet.

Politický aktivista – jeden z nejhorších kybernetických útočníků, protože se jedná zpravidla o znalce v oboru ICT, který prostřednictvím kyberprostoru reaguje na aktuální dění a politické problémy ve společnosti. Jedná se především o idealisty zastávající extrémní politické názory. Jejich útoky jsou směřovány proti politickým

konkurentům nebo vládním organizacím a jsou vedeny různorodě od obyčejného defacementu až po likvidaci informačních systémů oběti.[22]

2.2.2 Formy a způsoby kybernetických útoků v rámci kyberterorismu

Nástroje, principy a vývoj ICT přináší do světa kyberprostoru nepřeberné možnosti, což ostatně dokazuje i rozvoj internetu, počítačů, mobilních telefonů a dalších přístrojů. V době před dvaceti lety byla cena stolního počítače poměrně vysoká a pohybovala se v řádech deseti tisíců a mobilní telefon bylo těžké skrýt do kapsy, v krátkém období rozvoji ICT je výkon dnešních chytrých telefonů dvacetkrát vyšší než počítačů před patnácti léty. Díky rozvoji hardwaru je tak navýšen i výpočetní výkon pro rozvoj softwaru a vznikají mnohem komplexnější programová vybavení, které s sebou přináší i prostor pro vznik nástrojů, které nejsou vždy vytvořeny pro blaho uživatele. Většina softwaru pro kybernetický útok je šířena prostřednictvím dark webu, některé nástroje jsou dosažitelné i v běžném prostředí webu a díky rozvoji internetu nepotřebují tyto nástroje komplexnější znalosti ICT. Nástrojů pro kybernetický zločin je mnoho, ale využitelných nástrojů pro čistě kyberteroristický útok tuto skupinu podstatně zúží, neboť některé kybernetické nástroje jsou vytvořeny pouze pro podvody a generaci zisku nelegálním způsobem.

Jedním z obecných prostředků či nástrojů kybernetických útoků je malware (jedná se o spojení slov malicious software – škodlivý software). Je to všeobecně škodlivý software sloužící k narušení či zničení standartní činnosti počítačového systému, zisku dat, převzetí kontroly nad počítačovým systémem či přístupu do něj. Malware dále řadíme do různých skupin, které dělíme podle činnosti samotného škodlivého softwaru. I když jeden malware řadíme do skupiny podle jeho hlavní činnosti, můžeme se setkat s případy, že je schopen plnit několik funkcí naráz. Malware dělíme především na adware, spyware, viry (viruses), červy (worms), trojské koně (trojan horses), zadní vrátka (backdoor), rootkity, keyloggery, ransomware.

---

[22] JANOUŠEK, Michal, Kyberterorismus: Terorismus informační společnosti, In Obrana a strategie [online]. 20.03.2007, [cit. 2019-05-10]. Dostupné z WWW: <https://www.obranaastrategie.cz/filemanager/files/6513.pdf>

Pojem adware je slovní spojení „advertising supported software“, což znamená software pro podporu reklamy. Je jedním z méně nebezpečných, ale výdělečných forem malwaru, kdy uživateli zobrazuje reklamu na jeho počítačovém systému. Může mít další skryté funkce a to zejména jako spyware a sbírat tak data o činnosti uživatele a krást důležité informace.

Spyware je slovní spojení „spy software“, tedy špionážní software. Spyware shromažďuje data bez vědomí a souhlasu uživatele. Shromážděná data jsou následně odesílána na předem připravená datová shromaždiště. Spyware může být instalován jako samostatný malware, ale pravděpodobněji je součástí jiného programového balíčku, kde uživatel může nevědomky, aniž by si přečetl všeobecné podmínky užití, souhlasit také s instalací a chodem malwaru.

Viry, angl.. „viruses“, jsou škodlivé programy nebo části kódů, které jsou zpravidla navázány na jiný software nebo dokument. Jejich aktivace probíhá současně se spuštěním napadeného softwaru či dokumentu. Vir se sám reprodukuje a následně i šíří, tudíž nepotřebuje ke svému šíření součinnost uživatele. Existuje velká řada počítačových virů s různými funkcemi (schopnost šířit se a převzít kontrolu nad systémem, ničení systému, a další). Viry rozlišujeme podle cíle jejich útoku a to boot viry (napadají systémové oblasti), souborové viry (napadají soubory a obsah uživatele) a multiparitní viry (napadají systémové oblasti společně se soubory) a makro viry (napadají aplikace pomocí maker).

Červi, angl.. „Worms“, tato skupina malware je někdy zahrnována mezi viry. Na rozdíl od virů však červi nepotřebují spustitelný soubor, na který by byli navázáni. Šíří se zpravidla samostatně a využívají napadený systém k rozesílání dalších kopií sebe sama do dalších systémů za pomoci síťové komunikace. Červi se tímto způsobem mohou rychle šířit a tím zablokovat síťovou komunikaci nebo celé infrastruktury. Červi jsou schopni vyhledávat mezery v zabezpečení napadeného systému a využívat je. Tato vlastnost je zhodnocena reverzními inženýry k vyhledávání slabin systému a k jejich fixaci.

Trojské koně, angl. Trojan horses, jsou počítačové programy nebo kódy, které obsahují skryté funkce a mohou být nebezpečné pro samotné fungování systému. Trojské koně mohou být navázány na jiné programy nebo to může být program samotný, se skrytými funkcemi. Na rozdíl od viru se trojský kůň sám nereplikuje bez pomoci uživatele

(útočníka). Trojské koně jsou většinou aktivovány spuštěním programu, na který jsou navázány nebo podmíněnou akcí v systému. Po aktivaci mohou být funkce trojského koně různé, bývá využit k převzetí kontroly nad systémem, k mazání či poškození systému, ke kopírování dat, k instalaci dalšího malwaru nebo ke špionáži. Speciální formou trojského koně je tzv. „backdoor“ neboli zadní vrátka. Tento trojský kůň po aktivaci otvírá komunikační síťové porty napadeného systému a usnadňuje tak převzetí kontroly útočníkem nad napadeným systémem na dálku či instalaci dalšího malwaru nebo špionáže. Některý běžně dostupný a na první pohled bezpečný software obsahuje ve svém kódu také řetězce backdoor přístupu, který tam byl vložen úmyslně nebo se jedná o systémovou chybu. Tyto přístupy jsou někdy využity třetí stranou pro útoky na systém.

Dalším v řadě malwarů jsou rootkity. Jsou to počítačové programy a technologie sloužící k maskování přítomnosti a činnosti malwaru. Vyskytují se v podobě menších programů. Samotný rootkit není nebezpečný, ale většinou maskuje činnost mnohem nebezpečnějšího malwaru (trojský kůň, vir, červ, spyware). Rootkity upravují data a kódy programu nebo systému, tak aby nemohl reagovat na jiný malware či utají jeho existenci. Rootkity lze rozdělit do dvou skupin, první skupinou jsou systémové rootkity, které napadají a modifikují samotný operační systém a druhou skupinou jsou aplikační rootkity, které útočí a modifikují různé aplikace, kdy nejčastějším cílem jsou antivirové programy a firewally.

Dalším z řady malware je keylloger. Jedná se o software zaznamenávající činnost uživatele na klávesnici. Dalo by se říci, že tento software je podsystémem spywaru, ale díky jeho rozšíření, způsobu užití a specializací je v samostatné kategorii. Díky tomuto softwaru je útočník schopen získat názvy uživatelských účtů a hesla k nim z napadeného počítače a tyto dále využít ve svůj prospěch. Obecně se užívá k napadení počítače a získání přístupu k internetovému bankovnictví, různým sociálním službám pro krádeže identit nebo poškození uživatele, nebo jsou za pomoci různých výše uvedených malwarů distribuována do státních i nestátních organizací a následně užita ke špionáži nebo poškození organizace.

Posledním z řady malwaru je ransomware. Tento software využívají útočníci k vydírání oběti. Ransomware je do napadeného počítače nainstalován za pomoci trojského koně, viru nebo adwaru. Po aktivaci přebírá kontrolu nad systémem a systém

nebo vybraná data jsou zašifrována. Po uživateli je nejčastěji požadován finanční obnos a po té je systém dešifrován. [23]

Další sadou nástrojů pro kybernetický útok je mimo malware také DoS útok a jeho varianty DDoS a DRDoS. Pojem DoS je vlastně zkratkou k anglickému spojení slov „denial of service“, které v překladu znamenají odepření služby. Principem DoS útoku je přehlcení internetové služby a tím její zablokování pro ostatní uživatele. V některých případech dochází díky zahlcení systému k jeho pádu namísto pouhého zablokování. V případě DoS útoku je samotný útok veden pouze z jednoho zařízení a tomuto útoku se lze snadno ubránit blokací tohoto zařízení či komunikačního portu, na kterém zařízení s napadeným systémem komunikuje. Další variantou je DDoS (Distributed denial of service – překl. distribuované odepření služby) útok, který je veden současně z několika zařízení. Počet zařízení může být v řádech jednotek nebo tisíců, rozmístěných v různých geografických polohách. Proti DDoS útoku je velmi těžká obrana neboť je veden z více zařízení na více úrovních a je složité tyto útoky odklonit nebo blokovat. Pro tento způsob útoku je typické využití sítě botnetu. Tato síť je většinou tvořena různým počtem počítačových zařízení, nad kterými útočník přebírá kontrolu za pomoci malwaru a posléze celou síť využije k DDoS útoku. Poslední varianta je DRDoS (Distributed reflected denial of service – překl. distribuované odražené popření služby) útoku. Tento způsob útoku je proveden tak, že útočící systém vyšle zamaskovaný požadavek na server s maskovanou zpáteční adresou. Přepsaná adresa je adresou cíle útoku, dotazovaný server nebo počítačový systém na požadavek odpoví, ale svou odpověď odešle na adresu oběti, kdy ji nedobrovolně začne zahlcovat. Útočníkem se stává nedobrovolně dotazovaný systém. V případě DoS útoků není tedy cílem vniknutí do počítačového systému ale jeho vyřazení z provozu nebo omezení služeb. V některých případech by mohlo vyřazením strategicky důležitých služeb nastat ohrožení infrastruktury, majetku a v neposlední řadě lidských životů.[24]

[23] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. s. 204-221

[24] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. s. 295-305

2.2.3 Cíle kyberteroristických útoků

Pokud vezmeme v úvahu rychlost vývoje ICT a jejich aplikaci do každodenního života, můžeme očekávat, že možné cíle kybernetických útoků se rozšiřují stejně rychle. Cíle kybernetického terorismu budou voleny útočníky zejména tak, aby mohla relativně malá skupina nebo jedinec za užití co nejmenších zdrojů, napáchat největší možné škody a ztráty v civilním sektoru. V dnešní době, kdy je dostupnost i pokročilejších nástrojů pro méně odborné jedince veliká, je možné sledovat trend narůstajících kybernetických útoků.[25] Je velmi pravděpodobné, že v budoucnu mohou být cílem kybernetických útoků následující informační struktury:

- Distribuční soustavy elektrické energie – v této soustavě se mohou stát cílem zejména uzly distribuční soustavy ovládané dálkově, ale také samotná výrobní zařízení s cílem vyvolat lokální nebo celkový blackout.
- Distribuční soustava pitné vody – v této soustavě se mohou stát cíli kybernetického útoku čistírny vod, distribuční uzle ovládané dálkově, senzory distribuční sítě. V případě úspěšného útoku může být ochromena distribuce pitné vody, ale také i odvod splaškové vody.
- Ropný průmysl a jeho distribuční soustava – samotná distribuční soustava je závislá na dálkovém řízení a různých senzorech a v případě ohrožení nebo jejich vyřazení může přerušení dodávky ropných produktů ohrozit další mnohá odvětví průmyslu.
- Bankovní systémy – celá infrastruktura bankovních i nebankovních finančních společností je založena na ICT a je jejím prostřednictvím kontrolována a řízena. V případě úspěšného útoku může dojít k ochromení celosvětové ekonomiky. Tato infrastruktura je napadána spíše ze strany zločinců majících za cíl obohatit se, a proto je v této oblasti kladen značný důraz na bezpečnost.
- IOT – dalším z možných cílů jsou předměty napojené a řízené prostřednictvím internetu neboli „internet of things“ tedy internet věcí. Jejich využití a obliba v současnosti stále roste. Napojení a řízení kupříkladu vytápění objektu přes internetovou službu není v dnešní době nic výjimečného. V průmyslu jsou

[25] Rok 2019 bude ve znamení sofistikovanějších bezpečnostních útoků, SecurityWorld [online], 26.12.2018, [cit. 2019-05-30], dostupné na WWW: <https://computerworld.cz/securityworld/rok-2019-bude-ve-znameni-sofistikovanejsich-bezpecnostnich-utoku-55111

rozvíjeny technologie na dálkové ovládání strojů, vozidel a jiného zařízení. Převzetí kontroly nad takto vzdáleně ovládanými systémy může mít v budoucnu nebezpečný dopad na bezpečnost.

- Systémy veřejné správy – v neposlední řadě je také nutné uvést systémy veřejné správy. Tyto systémy jsou neustále pod tlakem kybernetických útoků. Vyřazením některých důležitých systémů by mohlo dojít k ohrožení bezpečnosti státu, kritické infrastruktury a osob vedoucí k možné paralýze ekonomiky a infrastruktury.

3 PRÁVNÍ OCHRANA PŘED KYBERNETICKÝM TERORISMEM V ČESKÉ REPUBLICE

3.1 Analýza norem České republiky souvisejících s kyberprostorem

V bezprostřední návaznosti na vznik a vývoj kyberprostoru musí státní aparát také reagovat na možné hrozby a nebezpečí související s tímto novým fenoménem. Pro samotnou dílčí ochranu jsou některé regulace zakotveny v různých zákonech, neboť kyberprostor je pro většinu styků, transakcí a procesů jen prostředkem k jejich sjednání nebo fungování. Pro mnohé se však kyberprostor stává samotným prostorem jejich vzniků a bytí. A v této rovině nastává potřeba ochrany a regulace některých jevů, které v přemíře mohou být škodlivé. V návaznosti na to vznikají a jsou novelizovány některé klíčové zákony vztahující se na kyberprostor a snažící se naplnit vznikající potřebu.

V souvislosti s kybernetickou trestnou činností a kybernetickou bezpečností je níže uveden seznam právních norem ČR, které mají bezprostřední vztah k této problematice:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích

- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Dále je zde nutné uvést také Ústavu a Listinu základních práv a svobod, které jsou prameny všech výše uvedených norem a zajišťují volný přístup k ICT a nakládání s prostředky ICT mimo případy, kdy je to zákonem zakázáno.

3.2 Trestně právní ochrana

V rámci roviny trestněprávního boje proti kyberterorismu je nutné stanovit, které konání je teroristickým činem, jak tokovému jednání předcházet, jak ho zjišťovat a potlačovat. Taxativním vyjmenováním jednání, které je trestným činem, se zabývá právě trestní zákoník v rovině trestního práva hmotného. Jak mají dotčené orgány činné v trestním řízení postupovat během vyšetřování těchto činů, jejich oprávnění a povinnosti k zajištění potřebných důkazů, popřípadě oprávnění k preventivním zásahům stanovuje právě trestní řád v rovině procesně právní.

Trestní zákoník stanovuje ve své zvláštní části, co je teroristickým činem ve skutkové podstatě níže uvedeného trestného činu:

§ 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) zničí nebo poškodí ve větší míře veřejné prostranství, majetek nebo veřejné zařízení, dopravní nebo telekomunikační systém, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, včetně počítačového systému, na jehož fungování takové zařízení, systém nebo plošina závisejí, s cílem vydat majetek v nebezpečí škody velkého rozsahu,

b) naruší nebo přeruší dodávku vody, elektrické energie nebo jiného základního přírodního zdroje s cílem vydat majetek v nebezpečí škody velkého rozsahu,

c) 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 anebo sdělí důležitou nepravdivou informaci, čímž vydá majetek v nebezpečí škody velkého rozsahu,

d) vydá 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 nebezpečí zvýší nebo ztíží jeho odvrácení nebo zmírnění, nebo

e) vložením dat do počítačového systému nebo na nosič informací anebo vymazáním nebo jiným zničením, poškozením, změněním nebo potlačením dat uložených v počítačovém systému nebo na nosiči informací, snížením jejich kvality nebo učiněním jich neupotřebitelnými provede útok proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok anebo útok, kterým způsobí značnou škodu,

(2) 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 prostranství, majetek nebo veřejné zařízení, dopravní nebo telekomunikační systém, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, včetně počítačového systému, na jehož fungování takové zařízení, systém nebo plošina závisejí, s cílem ohrozit tím lidské životy nebo bezpečnost takového prostranství, zařízení, systému nebo plošiny,

d) naruší nebo přeruší dodávku vody, elektrické energie nebo jiného základního přírodního zdroje s cílem ohrozit tím lidské životy,

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 anebo sdělí důležitou nepravdivou informaci, čímž ohrozí život nebo zdraví lidí nebo bezpečnost takového dopravního prostředku,

f) vyrábí nebo jinak získá, přechovává, dováží, přepravuje, vyváží či jinak dodává nebo užije výbušninu, jaderný materiál, jadernou, biologickou, chemickou nebo jinou zbraň, bojový prostředek nebo materiál obdobné povahy, anebo provádí výzkum a vývoj jaderné, biologické, chemické nebo jiné zbraně nebo bojového prostředku nebo výbušniny, nebo

g) vydá lidi v obecné nebezpečí smrti nebo těžké újmy na zdraví 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.[26]

Výše uvedená skutková podstata je koncipována takovým způsobem a také pro takové případy, že je možné postihnout také jednání teroristů v kyberprostoru, protože skutková podstata trestného činu teroristického útoku zahrnuje i útok na telekomunikační sítě a další možné cíle, na které mohou být vedeny útoky v kyberprostoru. Teroristé se také v souvislosti s kyberteroristickými útoky mohou dopustit i dalších trestných činů, pro příklad jsou zde uvedeny některé skutkové podstaty těchto trestných činů:

§ 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,

§ 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

[26] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 394 - 406. Dostupné z WWW:< https://www.zakonyprolidi.cz/cs/2009-40 >

(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.[27]

Níže jsou uvedeny další trestné činy související s terorismem:

§ 175 Vydírání,

§ 312 Teror,

§ 312a Účast na teroristické skupině,

§ 312d Financování terorismu,

§312e Podpora a propagace terorismu,

§ 312f Vyhrožování teroristickým trestným činem,

§ 314 Sabotáž,

§ 276 Poškození a ohrožení provozu obecně prospěšného zařízení.

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob,

---

[27] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 394 - 406. Dostupné z WWW:< https://www.zakonyprolidi.cz/cs/2009-40 >

§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod,

§ 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,

§ 407 Podněcování útočné války.[28]

Oprávnění a povinnosti orgánů činných v trestním řízení při vyšetřování a předcházení trestné činnosti, v tomto případě trestných činů souvisejících s kyberterorismem, jsou uvedeny v trestním řádu. Je zde upraven zejména postup pro zajištění elektronické komunikace a elektronického provozu. V první části trestního řádu v hlavě čtvrté v sedmém oddílu je část pojednávající o odposlechu a záznamu telekomunikačního provozu v § 88 a v § 88a trestního řádu sloužícího k odhalování a zajišťování důkazních prostředků v souvislosti s telekomunikačním provozem. V rámci dalších možností mohou k odhalování a šetření kybernetických trestných činů orgány činné v trestním řízení vyžadovat odborná vyjádření, znalecké posudky (§ 105 až § 11 TŘ) a ve složitějších případech může policejní orgán využít služeb konzultanta (§ 157 TŘ)[29]

Ačkoliv je současný trestní zákon koncipován dobře, je nutné uvést, že ve vztahu ke kybernetickým útokům má některé faktické mezery. Příkladem mohou být právě DoS útoky, na které je těžké aplikovat skutkovou podstatu současných trestných činů, neboť pokud se jimi nedopustí útočník dalších trestných činů, sami o sobě nejsou trestným činem, protože nepřekonávají žádné bezpečností opatření a nevnikají do žádného systému, pouze slouží k zablokování služby. Bylo by dobré v rámci úvah de lege ferenda toto jednání zahrnout mezi trestné činy, neboť blokováním internetových služeb mohou vznikat obětem nemalé škody a v některých případech může dojít k vážnějšímu ohrožení bezpečnosti.

---

[28] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 394 - 406. Dostupné z WWW:< https://www.zakonyprolidi.cz/cs/2009-40 >

[29] ČESKO. Zákon č. 141/1961 Sb., trestní řád. In Sbírka zákonů, Československá socialistická republika. 1961, částka 66, s. 513 - 576. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/1961-141#cast2 >

3.3 Zákon o kybernetické bezpečnosti

Další normou ČR k ochraně před kybernetickými útoky je zákon o kybernetické bezpečnosti. Tento zákon je důležitým legislativním krokem ke zvýšení bezpečnosti kybernetického prostoru a ochraně kritické infrastruktury před kybernetickými útoky. Zákon byl schválen dne 23.07.2014, účinnost nabyl dne 01.01.2015 a jeho celý název zní zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákon o kybernetické bezpečnosti neřeší obecně trestnou činnost v kybernetickém prostoru, ale svým zaměřením se věnuje prevenci před bezpečnostními hrozbami a reakcí na vzniklé nebezpečí v kyberprostoru. Je první normou, která definuje pojmy jako kybernetický prostor a kritická informační struktura. Dále zákon zřizuje národní tým CERT (computer emergency rosponse team), který působí na poli ochrany a prevence v rámci kritické informační struktury a významných informačních systémů[30,31].

[30] ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2014-181#redakce>

[31] GovCert.cz, Národní centrum kybernetické bezpečnosti [online], [cit. 2019-06-25], dostupné na WWW: <https://www.govcert.cz/cs/vladni-cert/govcert-cz/>

4 MEZINÁRODNÍ PRÁVNÍ OCHRANA PŘED KYBERNETICKÝM TERORISMEM

4.1 Ochrana v rámci EU

Po událostech dne 11.09.2001 v New Yorku je hrozba terorismu vnímána jako celosvětový problém a nebezpečí pro obyvatele. Rada EU pro spravedlnost a vnitřní věci přijímá v reakci na tento útok Akční plán boje proti terorismu. Postupným politickým vývojem a reakcí na další teroristické útoky vně území EU dospívá v roce 2005 rada k přijetí Strategie EU pro boj proti terorismu. Tato strategie je založena na čtyřech pilířích, kterými jsou prevence, ochrana, pronásledování, reakce. Strategie je doplňována akčními plány a dalšími úmluvami, ale její principy jsou dodržovány do současnosti. V návaznosti na stále častější útoky byl v lednu roku 2016 spuštěn provoz Evropského protiteroristického centra pod správou Europolu. Centrum pomáhá sdílet informace mezi členskými státy a podílí se na prevenci a vyšetřování terorismu.

V oblasti kyberkriminality schvaluje dne 08.11.2001 Výbor ministrů rady EU Úmluvu Rady Evropy č. 185 o kyberkriminalitě, která vstupuje v platnost dne 01.07.2004. Česká republika úmluvu podepisuje dne 09.02.2005 a k ratifikaci dochází dne 22.08.2013, v platnost na území České republiky vstoupila dne 01.12.2013. Úmluva o kyberkriminalitě byla také podepsána a ratifikována státy jako je USA a Japonsko. Jedná se o historicky a právně významný dokument sjednocující národní právní úpravy v oblasti kyberkriminality. Úmluva o kyberkriminalitě stanovuje smluvním stranám povinnost implementovat do jednotlivých národních právních norem nástroje, pojmy a postupy, aby bylo možné jasně definovat jednotlivé skutkové podstaty kybernetických trestných činů, možnost aplikace norem v kyberporstoru a stanovit jednotný postup proti pachatelům těchto činů. Úmluva o kyberkriminalitě je složena z preambule a 48 článků rozdělených do čtyřech kapitol:

1) Používané pojmy

2) Opatření, která mají být přijata na vnitrostátní úrovni

- Část 1 – Trestní právo hmotné
- Část 2 – Procesní právo

- Část 3 – Soudní pravomoc

3) Mezinárodní spolupráce

- *Část 1 – Obecné zásady*
- *Část 2 – Zvláštní ustanovení*

4) Závěrečná ustanovení[32]

V rámci Úmluvy o kyberkriminalitě byly definovány čtyři základní skupiny trestných činů, které jsou významným krokem ke sjednocení práva. Zakotvením těchto obecných institutů do trestního práva hmotného a jednotné definování kybernetických útoků umožňuje jejich efektivnější odhalování, potírání a předcházení. Úmluva o kyberkriminalitě dělí trestné činy do těchto skupin:

- Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů;
- Trestné činy související s počítači;
- Trestné činy související s obsahem;
- Trestné činy související s porušováním autorských práv a souvisejících práv.

Dne 28.01.2003 byl přijat dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě. Dodatek se věnuje okruhu trestných činů spočívajících v šíření určitého závadového obsahu. Specificky se jedná o materiál se zaměřením xenofobního, rasistického či jinak projevujícího nesnášenlivost projevu. Vzhledem ke skutečnosti, že USA podepsalo a ratifikovalo Úmluvu o kyberkriminalitě, nebyla některá ustanovení, která se objevují v dodatku do samotné zahrnuta, neboť některé rasistické či xenofobní projevy nejsou v USA považovány za trestný čin a z pohledu jejich Ústavy by se jednalo o omezení svobody projevu. Dodatkový protokol

[32]KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. s. 332-333

k Úmluvě o kyberkriminalitě se skládá z preambule a 16 článků, které jsou rozděleny do čtyř kapitol:

1) Obecná ustanovení;
2) Opatření, která mají být přijata na vnitrostátní úrovni:
   a) Šíření rasistického a xenofobního materiálu skrze počítačový systém,
   b) Rasisticky a xenofobně motivovaná výhružka,
   c) Rasisticky a xenofobně motivovaná urážka,
   d) Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy;
3) Vztah mezi Úmluvou o kyberkriminalitě a Dodatkovým protokolem;
4) Závěrečná ustanovení.

Na základě důležitosti mezinárodní spolupráce a sjednocení pojmosloví i postupů v rámci potírání kyberkriminality jsou v rámci EU využity prostředky pro sblížení národních práv, zejména rámcová rozhodnutí, směrnice a další dokumenty EU a ES.

Z pohledu boje s kyberkriminalitou a kybernetickým terorismem jsou nejvýznamnějšími následující dokumenty:

- Směrnice Rady 91/250/EHS o právní ochraně počítačových programů
- Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů
- Směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informaci v oblasti norem a technických předpisů ve zněni směrnice č. 98/48/ES
- Směrnice č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)
- Směrnice Evropského parlamentu a Rady č. 2002/21/EC o společném regulačním rámci pro sítě a služby elektronických komunikací („rámcová směrnice“)
- Směrnice Evropského parlamentu a Rady č. 2002/19/EC o přístupu k sítím elektronických komunikaci a přidruženým zařízením a o jejich propojeni („přístupová směrnice“)

- Směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávněná pro sítě a služby elektronických komunikaci („autorizační směrnice“)
- Směrnice Evropského parlamentu a Rady č. 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikaci („směrnice o universální službě“)
- Směrnice Evropského parlamentu a Rady 2002/58/EC tykající se zpracovávaní osobních údajů a ochrany soukromí v oblasti elektronických komunikaci („směrnice o ochraně údajů v elektronických komunikacích“)
- Směrnice Komise č. 2002/77/ES o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami („soutěžní směrnice“)
- Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávaní mezi členskými státy
- Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů - Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) ze dne 15. 11. 2006
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22.05.2007
- Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti ze dne 27. listopadu 2008
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ ze dne 30. 3. 2009
- Sdělení komise Radě a Evropskému parlamentu, Řešeni trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě. 2012
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013, o Agentuře Evropské unie pro bezpečnost siti a informaci (ENISA) a o zrušeni nařízení (ES) č. 460/2004, ze dne 21. května 2013

- Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy a nahrazeni rámcového rozhodnuti Rady 2005/222/SVV, ze dne 12. srpna 2013
- Nařízení Evropského parlamentu a Rady (EU) č. 513/2014, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nastroj pro finanční podporu policejní spolupráce, předcházení trestné činnosti, boje proti trestné činnosti a řešeni krizí a zrušuje rozhodnuti Rady 2007/125/SVV, ze dne 16. dubna 2014
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušeni směrnice 1999/93/ES, ze dne 23. července 2014
- Nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazovaní pravá (Europol) a o zrušeni a nahrazeni rozhodnuti 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. května 2016
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracovaným osobních údajů a o volnem pohybu těchto údajů a o zrušeni směrnice 95/46/ES („obecné nařízení o ochraně osobních údajů“)
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištěni vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, ze dne 6. července 2016 (NIS Directive)[33]

4.2 Ochrana v rámci NATO

V rámci mezinárodního práva vztahujícího se na oblast kyberprostoru byl vydán prostřednictvím Centra excelence pro spolupráci v oblasti kybernetické obrany NATO v březnu roku 2013 Tallinský manuál mezinárodního práva použitelného na kybernetickou válku. Ačkoliv je manuál směřován do odvětví kybernetické války, jeho dopady jsou mnohem širší. V zásadě stanovuje, že mezinárodní právo v oblasti kybernetického prostoru není odlišné od fyzického světa či fyzického území jednotlivých států, kdy každý stát má svůj vlastní kyberprostor, za který je

[33] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8. s. 335-337

zodpovědný. Je zde také stanoveno, že pro kybernetický prostor nemusí být stanovena žádná zvláštní pravidla jako kupříkladu pro mezinárodní vody. Ačkoliv státy jako Ruská federace, Čína a další usilovně jednají a navrhují regulaci kyberprostoru, je mimo Úmluvu o kyberkriminalitě jedinou dosavadní mezinárodní uznávanou regulí kyberprostoru uvedený Tallinský manuál.[34]

[34] FLÍDR, Tomáš, Mezinárodní právo v kyberprotoru a Tallinský manuál, Kyberbezpečnost, 22.11.2013 [online]. 22.11.2013, [cit. 2019-07-01]. dostupné na WWW: <https://www.kyberbezpecnost.cz/?p=198>

5 PŘÍPADOVÉ STUDIE

5.1 Kritéria hodnocení případových studií

Pro samotné vyhodnocení případových studií je nezbytné stanovit kritéria hodnocení, na jejíchž základě je možné vyhodnotit daný případ, zda se jedná o kybernetický terorismus nebo pouze o kybernetický útok. Kritéria jsou volena na základě zpracovaných informací a definicí uvedených v předchozích kapitolách této práce, kde byl definován teroristický a kyberteroristický čin.

5.1.1 Cíle a následky

Toto kritérium vychází ze samotné definice terorismu, kdy je útok veden proti civilnímu obyvatelstvu a kritické infrastruktuře a dalším nezúčastněným objektům s cílem vytvořit psychologický nátlak na společnost vedoucí ke změně chování nebo vytvoření nátlaku na vládnoucí aparát a vyvolání obavy z opakovaného útoku.

5.1.2 Způsob útoku

Dalším zvoleným kritériem je způsob vedení samotného útoku. Pro správné zařazení mezi teroristické útoky je nutné, aby samotný útok byl proveden veřejně a měl jasné poselství.

5.1.3 Forma útoku

Forma nebo také užité nástroje jsou důležitým kritériem pro analýzu a následné zhodnocení jednotlivých případů. Aby bylo možné samotný útok odlišit od konvenčního útoku a zařadit ho mezi kybernetické útoky, musí být veden proti informační struktuře či kritické infrastruktuře za užití kybernetických nástrojů či zbraní.

5.1.4 Aktéři

Posledním kritériem je určení aktérů samotného útoku. Samotný teroristický nebo kyberteroristický útok jak už bylo uvedeno výše je proveden veřejně a má jasné poselství, které definuje útočník (politické, náboženské a další). Je tedy nezbytné, aby byl útočník známý a ke svým činům se přihlásil. Nejčastějšími aktéry jsou jedinci, skupiny či organizace s náboženským či politickým radikálním smýšlením.

5.1.5 Způsob vyhodnocení

Pro přehlednost bude v rámci analýzy každé případové studie vytvořena tabulka, kde budou zhodnocena jednotlivá výše uvedená kritéria a na základě těchto kritérií budou vybrané případy kybernetických útoků vyhodnoceny.

Cíle a následek	
Způsob	
Forma	
Útočníci	

Tabulka č. 1 – Modelová tabulka pro analýzu konfliktu

5.2 Estonsko-ruský konflikt

5.2.1 Stručné shrnutí konfliktu

Celý konflikt vznikl v roce 2007, kdy už tak napjatý vztah mezi Estonskem a Ruskou federací vygradoval přesunem sovětského válečného památníku neznámého vojáka ve městě Tallinn. Rusko v reakci na tento přesun provedlo blokádu estonské ambasády a začalo se jednat i o ekonomických sankcích. V poměrně krátké době odstartovala vlna kybernetických útoků cílených proti estonským vládním webům, bankám a médiím. Kybernetický útok lze členit na dvě fáze. První fáze probíhala v období od 27.04.2007 do 29.04.2007, tato fáze se vyznačovala nepříliš vysokou úrovní propracovanosti a byla označena názvem „emocionální odezva“, cílem útoků byly zejména vládní webové stránky a stránky zpravodajských médií. Druhá fáze útoků probíhala v období od 30.04.2007 do 18.05.2007. Tato fáze se vyznačovala mnohem propracovanějšími, koordinovanějšími a sofistikovanějšími útoky. Během incidentu byly využity DDoS útoky vedené z několika míst na světě a dobře maskované. Tato fáze měla čtyři vlny:

- První vlna přišla 04.05.2007 za pomoci DDoS útoků s globálními botnety, které cílily na webové stránky a DNS servery vládních organizací. Během tohoto útoku byly některé servery vyřazeny z provozu a dočasně nedostupné.

- Druhá vlna přišla ve dnech 09.05.2007 až 11.05.2007. Ke Dni vítězství (09.05.2007), se kterým bylo spojeno i odstranění památníku, byly útoky očekávány. Příchozí DDoS útoky vyřadily z provozu 58 stránek, mezi které patřily zejména vládní stránky. V období druhé vlny zaznamenaly také bankovní servery DDoS útoky, které vyřadily jejich služby na několik hodin z provozu.
- Třetí vlna přišla dne 15.05.2007. DDoS útoky jsou vedeny z rozsáhlého botnetu zahrnujícího přibližně 85000 zapojených počítačů. Útoky mířily proti vládním serverům a mimo to také odstavily portál banky SED Eesti a několika dalších.

Po celou dobu konfliktu byly cílem servery a služby významných estonských vládních organizací, konkrétněji ministerstvo obrany, ministerstvo zahraničí a taktéž i významná estonská média.

V rámci zjištěných skutečností, které byly zveřejněny a to zejména adresy IP útočníků, bylo zjištěno, že část jich směřuje na počítače ruských úředníků i z vyšších úřadů. Z celého útoku tedy bylo nejprve podezřelé Rusko, avšak podezření se nijak nepotvrdilo a Rusko odmítlo účast na tomto útoku a jeho účast se nepodařilo prokázat. Za hlavní iniciátory byli označeni ruští hackeři, neboť se podařilo prokázat, že původ útoků je v Rusku. [35]

[35] PAVLÍKOVÁ, Miroslava, Estonsko-ruský incident v kontextu kyberterorismu, Global Politics [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW: <http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu>

5.2.2 Analýza konfliktu

Cíl a následek	Cílem útoku se staly především vládní servery a vládní webové stránky, následovány byly i servery a webové stránky předních médií a bankovních institucí. Během incidentu došlo k rozsáhlým výpadkům služeb, nedošlo k ohrožení života či změně nálady obyvatelstva nebo vyvolání strachu.
Způsob	Útok je veden na informační média vládních i nevládních organizací, kdy však útočník či útočící skupina se k samotnému útoku nehlásí a není jasně dané poslání samotného útoku, ačkoliv z předešlých událostí vyplývá, že útok byl veden jako odveta za přesunutí památníku.
Forma	Útoky jsou vedené kybernetickými nástroji (DDoS útok prostřednictvím botnetů) v kybernetickém prostoru.
Útočníci	Přesně nezjištěná nevládní organizace ruských hackerů, která se nikdy k útoku nepřihlásila.

Tabulka č. 2 – analýza Rusko-Gruzínského konfliktu

5.2.3 Vyhodnocení konfliktu

Z analýzy celého konfliktu vyplývá, že ačkoliv je útok veden prostřednictvím kybernetických nástrojů, v tomto případě DDoS útok, v kyberprostoru a jeho cílem je informační struktura vládních i nevládních organizací, nemůžeme tento konflikt zařadit do kategorie kybernetických teroristických činů. Jedním z hlavních důvodů, proč konflikt nelze zařadit mezi akty kyberterorismu je, že útok je sice domnělou reakcí na přesun památníku, ale nevysílá jasné poselství a jeho intenzita a následky nemají zřejmý vliv na náladu civilního obyvatelstva a nemají požadovaný

psychologický účinek, dokonce nezpůsobil ani ztráty na životech či jejich ohrožení. Dalším důvodem je, že celý útok provedla skupina, která se nesnaží sama sebe a svůj čin propagovat a ani se k němu nehlásí, naopak se snaží svou identitu ukrýt, proto nelze zjistit přesná motivace k útoku. Následky v reálném světě jsou spíše pozitivní a díky tomuto konfliktu jsou zřizovány kybernetické bezpečností organizace na různých úrovních od mezinárodních až po národní.

5.3 Stuxnet – útok na jadernou elektrárnu v Íránu

5.3.1 Stručné shrnutí konfliktu

V lednu v roce 2010, při rutinní kontrole bylo v Íránském zařízení pro obohacování uranu v Natanz zjištěno, že část centrifug nefunguje správně. Kontrolou kamerových záznamů a zpětnou analýzou chodu zařízení pracovníci zjistili, že dochází k nadměrnému opotřebení zařízení a jeho nahrazování oproti datům zjištěným minulým provozem. Příčina byla zjištěna až v červnu roku 2010, kdy zaměstnanci společnosti VirusBlockAda zjistili přítomnost neznámého malwaru v notebooku jejich íránského zákazníka. Z profesionálního hlediska se jednalo o velice sofistikovaný a složitý malware. Stuxnet je druh červa, který byl přesně cílený na součástky průmyslových ovladačů společnosti Siemens, které záměrně poškozoval. Tomuto malwaru byl přiřazen název „STUXNET“. Podle zjištěných rozborů kódů se šířil za pomoci chyb a slepých míst v softwaru Windows prostřednictvím USB flash disků a svoji přítomnost dokázal dokonale skrýt před antivirovým softwarem, protože se instaloval zároveň jako rootkit. Popis Stuxnetu na serveru root.cz vcelku přesně definuje jeho užití a složitost jeho syntaxe:

„I v případě systémů Siemens byl ale Stuxnet napsán doslova jako práce softwarového odstřelovače. Vybíral si totiž jen PLC systémy s ovládacím rozhraním od dvou výrobců z Finska a Íránu a útočil výhradně na ty ovládající motory s rychlostí otáček mezi 807 a 1210 Hz – ty jsou používány prakticky výhradně u pump a plynových centrifug. Při splnění určitých podmínek pak Stuxnet nejprve zvyšuje otáčky centrifug ze standardních 1064 Hz na nadlimitních 1410 Hz po dobu 15 minut a po necelém měsíci naopak otáčky sníží až na 100–200 Hz na 50 minut (cílem je centrifugy nenápadně poškodit a odstavit z provozu). Zároveň se instaluje jako rootkit, aby mohl maskovat

svou přítomnost a činnost – například tak, že sděluje připojeným monitorovacím systémům fiktivní údaje, podle nichž se zdá, že se nic podezřelého neděje.“[36]

Původce viru nebyl nikdy oficiálně odhalen a přesný zdroj nákazy íránského zařízení také nebyl nikdy zjištěn. Přesnou analýzou se však podařilo zjistit, že celý software byl výhradně cílený na íránská jaderná zařízení a jednalo se o velmi sofistikovanou kybernetickou zbraň. V podstatě pokud vezmeme v úvahu odpor Izraele a USA proti íránskému jadernému programu, tak jsou tyto dvě země jako původci Stuxnetu velmi nasnadě. V rámci spekulací je možné, že původcem viru je právě USA a jejich program pro vývoj kybernetických nástrojů a zbraní pod názvem „Olympijské hry“, což však nebylo nikdy veřejně přiznáno ani dokázáno. [37]

[36] ERBEN, Lukáš, Příchod hackerů: Příběh Stuxnetu, In root.cz [online]. 29.04.2014, [cit. 2019-06-10]., dostupné na WWW: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>

[37] ERBEN, Lukáš, Příchod hackerů: Příběh Stuxnetu, In root.cz [online]. 29.04.2014, [cit. 2019-06-10]., dostupné na WWW: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>

5.3.2 Analýza konfliktu

Cíl a následek	Cílem samotného útoku bylo jaderné zařízení v Íránu v Natanz a další možná zařízení využívající specifický hardware Siemens. Během incidentu bylo soustavně poškozováno Íránské jaderné zařízení prostřednictvím softwarového útoku v průběhu několika měsíců až několika let.
Způsob	Kybernetický útok byl v utajení, aby mohl být útočný software, co nejdéle aktivní. V rámci útoku byla velká snaha o maskování malwaru a k útoku se oficiálně nepřiznala žádná skupina či organizace.
Forma	Útok byl veden prostřednictvím velmi sofistikovaného malwaru vytvořeného proti vybavení jaderného zařízení především v Íránu. Jednalo se o druh červa s vlastnostmi dalšího malwaru (rootkit, spyware).
Útočníci	K útoku se nepřihlásila žádná organizace či skupina. Podle zjištěných skutečností je velice pravděpodobné, že Stuxnet byl vyvíjen jako kybernetická zbraň a za jeho vznikem může stát vládní organizace.

Tabulka č.3 – Analýza útoku malwarem STUXNET

5.3.3 Vyhodnocení konfliktu

Na základě výše provedené analýzy je možné útok na íránské jaderné zařízení hodnotit jako vysoce sofistikovaný kybernetický útok, ale nejedná se o kybernetický terorismus. Proti zařazení tohoto útoku mezi kyberterorismus vypovídají zejména skutečnosti, kterými jsou i to, že celý útok je veden v maximálním možném utajení,

k samotnému útoku se nepřihlásila žádná skupina či organizace a nevydává tím žádné poselství a cílem útoku nebylo ani ovlivnění nálady obyvatelstva nebo vytvoření psychologického nátlaku, ale vyřazení jaderného zařízení z provozu. Celý útok se jeví jako vysoce kvalifikovaná vojenská diverzní operace.

Důsledkem tohoto útoku bylo, že země na Blízkém východě začaly brát svou kybernetickou bezpečnost velmi vážně a zpřísnily svou kybernetickou ochranu. Civilní obyvatelstvo nebylo tímto útokem zasaženo.[38]

5.4 Kybernetický útok malwarem Flame

5.4.1 Stručné shrnutí konfliktu

V průběhu roku 2012 a v reakci na předešlý kybernetický útok prostřednictvím malwaru Stuxnet země na Blízkém východě posílily svoji bezpečnost, a tak byla zachycena nová hrozba. V počítačích íránského ministerstva ropného průmyslu byl společností Kaspersky Lab zjištěn malware připomínající svou syntaxí a způsobem napadání softwarového červa Stuxnet. Analýzou jeho kódu bylo zjištěno, že se jedná o jednu z největších bezpečnostních hrozeb v uvedené době, neboť tento software byl ještě sofistikovanější a hůře odhalitelný než Stuxnet. Tento malware řadící se mezi červy s prvky spywaru a rootkitu byl nazván „FLAME“. Flame sám o sobě necílil na zničení hardwaru jako Stuxnet, ale infiltroval se do počítače velmi sofistikovaným složitým způsobem prostřednictvím emailové korespondence nebo USB disků, aniž by byl zachycen jakýmkoliv bezpečnostním softwarem. Po své aktivaci shromažďoval uživatelská data a odesílal je na předem dané adresy, jednalo se o velmi rozsáhlé datové skupiny od dokumentů, přes obrázky až po uložené výkresy v různých formátech. Flame byl dokonce schopný vytvářet screen obrazovky a pořizovat fotografie a videozáznamy prostřednictvím připojeného periferního zařízení nebo integrované kamery. Flame sám o sobě také působil jako keylogger. V rámci působení byl Flame zjištěn převážně v počítačových systémech zemí jako Írán, Palestina, Sýrie, Izrael, Libanon, Saudská Arábie, Egypt, ale byly zjištěny i jednotlivé případy v zemích jako Rakousko, Rusko, Maďarsko a Hong Kong. Jak už bylo uvedeno Flame necílil na destrukci zařízení, ale jeho primárním cílem bylo shromažďování dat a jejich

[38]ERBEN, Lukáš, Příchod hackerů: Příběh Stuxnetu, In root.cz [online]. 13.05.2014, [cit. 2019-06-10]., dostupné na WWW: < https://www.root.cz/clanky/prichod-hackeru-operace-olympijske-hry/>

odesílání útočníkovi. Dalo by se říci, že to byl kybernetický vysavač průmyslových a strategických dat. Infikovány byly počítače nejrůznějších vlastníků od vysokoškolských zařízení až po počítačové systémy státních úřadů. Flame byl schopný se sám reprodukovat a následně se i šířit. Nejzajímavějším faktem zůstává, že samotný malware měl velikost 20 MB, což je vskutku na téměř neodhalitelného červa celkem úctyhodná velikost.[39]

[39] ERBEN, Lukáš, Příchod hackerů: Příběh Stuxnetu, In root.cz [online]. 13.05.2014, [cit. 2019-06-10]., dostupné na WWW: < https://www.root.cz/clanky/prichod-hackeru-operace-olympijske-hry/>

5.4.2 Analýza konfliktu

Cíl a následek	Cíle kybernetického útoku prostřednictvím malwaru Flame byly počítačové systémy vybraných zemí na Blízkém východě, především v Íránu. Během napadení nedošlo k vyřazení či ohrožení počítačového systému nebo informační struktury, byla pouze extrahována data a následně odeslána na připravená úložiště.
Způsob	Celý útok byl veden vysoce složitým a propracovaným malwarem - červem, který velice úspěšně tajil svoji přítomnost v napadeném zařízení. Útok byl veden tajně, k útoku se oficiálně nepřiznala žádná skupina či organizace a nepodařilo se nikdy oficiálně odhalit výrobce malwaru.
Forma	Útok byl veden prostřednictvím velmi sofistikovaného malwaru vytvořeného za účelem extrakce dat z počítačových systémů především v zemích Blízkého východu a jejich následného odeslání na předem připravená datová shromaždiště. Jednalo se o druh červa s vlastnostmi dalšího malwaru (rootkit, spyware).
Útočníci	K útoku se nepřihlásila žádná organizace či skupina. Podle zjištěných skutečností je velice pravděpodobné, že Flame stejně jako Stuxnet byl vyvíjen jako kybernetická zbraň a za jeho vznikem stojí vládní organizace.

Tabulka č. 4 – Analýza útoku malwarem FLAME

5.4.3 Vyhodnocení konfliktu

Analýzou útoku prostřednictvím malwaru Flame bylo zjištěno, že uvedený útok je pouze kybernetickým útokem, neboť postrádá všechny prvky teroristického jednání a to zejména, že není veden veřejně ale utajovaně, cílem je extrakce dat z počítačových systémů, útočník je neznámý, nedochází k ohrožení obyvatelstva ani psychickému nátlaku. Útok samotný je příkladem vojenské či špionážní operace provedené v kyberprostoru za užití vysoce sofistikovaného a účinného nástroje.

Následky z útoku Flame nejsou známy, neboť se nepodařilo zjistit jaké údaje byly z cílových počítačových systémů extrahovány a jakým způsobem byla tato data využita. Nicméně nedošlo k žádnému viditelnému následku ani v napadených počítačových systémech. V reakci na tyto útoky je celosvětový trend ve zvyšování kybernetické bezpečnosti. Malware Stuxnet i Flame měli své další nástupce jako Gauss, DuQu, Duqu 2, kteří také cílí na extrakci dat a u některých nástupců je možné sledovat jejich podobnost kódu se Stuxnetem a Flame.

5.5 Predikce vývoje kyberterorismu

Kybernetický terorismus, který byl definován v předešlých kapitolách, se v podstatě nevyskytuje. Teroristické skupiny raději volí konvenční prostředky ke svým útokům, vládou podporované organizace provádějí spíše tajné operace, tak aby nebyla zjištěna jejich přítomnost v napadeném systému a jednotlivci málokdy mají potřebné vybavení, motivaci a potencionál pro vedení úspěšného útoku na důležitější kybernetickou infrastrukturu. V současné době jsou více než teroristické útoky v kyberprostoru vedeny informační útoky a války mezi jednotlivými státy jako jsou USA a jejich příznivci a Rusko, Čína a další státy stojící na „opačné straně". Vývoj ICT je však velmi dynamický a vyspělý, svět je na těchto technologiích stále závislejší. Příkladem může být internet věcí, kdy je stále ve větší míře obyčejná technika řízena dálkově a automaticky. Dalším příkladem je revoluce v průmyslu tzv. „Průmysl 4.0", kdy se do výrobních procesů stále více implementuje výrobní technologie založená na bezobslužných strojích a robotických linkách řízených a kontrolovaných dálkově. Kritická infrastruktura a zejména distribuční systémy jsou řízeny dálkově ovládanými senzory a čerpadly. V přepravě jsou implementovány prvky umělé inteligence do automatických řídících systémů vozidel a jsou testovány bezobslužné přepravní jednotky – nákladní vozidla i osobní vozidla. Ve vojenském průmyslu jsou stále více zaváděny bezobslužné stroje a dálkově řízené stroje – bezpilotní letouny, drony, bezpilotní vozidla, automatické špionážní letouny. Trend vývoje bezobslužných či dálkově řízených strojů a zařízení je na vzestupu a zatím nejsou žádné indicie, že by ustupoval. Společně s tímto trendem a postupným zaváděním těchto technologií do běžného života však stoupá i riziko zneužití chyb a mezer v bezpečnosti těchto technologií ve prospěch zločinců a teroristů a také nepřátelských států. Je proto důležité, aby současně s technologickým vývojem stoupala i úroveň bezpečnosti v oblasti místní i mezinárodní legislativy, faktické bezpečnosti a povědomí uživatelů o bezpečnosti technologií a jejich možnostech.

Pokud se budeme hlouběji zabývat bezpečností a možným vznikem hrozeb v budoucnu, může být dobrým příkladem malware Stuxnet, který byl schopen napadnout uzavřený bezpečný systém bez přístupu k celosvětové síti Internetu a úspěšně převzít kontrolu nad zařízením a poškodit ho. Je jen otázkou času, kdy technická vyspělost naší civilizace dosáhne takové úrovně závislosti na moderních technologiích, že se technologická zařízení propojena pomocí kyberprostoru stanou

lákavými cíli pro různé teroristické skupiny a hnutí. Další otázkou je jaký dopad můžeme od těchto útoků očekávat. Neboť převzetí kontroly nad dálkově řízenými stroji, ať už bojovými nebo civilními může mít katastrofální následky, kupříkladu v podobě dálkově ovládaného stroje, který může kdekoliv a kdykoliv zaútočit. Další oblastí, kde můžou teroristé způsobit škody, jsou dálkové řízené systémy distribucí elektrické energie, vody, ropných produktů. Tyto distribuční soustavy jsou už dnes ovládány různými senzory a dálkově řízenými čerpadly a zařízeními. V případě převzetí kontroly nad senzory může dojít k vyřazení provozu a tím ohrožení kritické infrastruktury jednotlivých států.[40,41,42]

Také je nutno brát v potaz i vyšší úroveň znalostí dnešních uživatelů počítačových systémů, kdy každá další generace uživatelů je mnohem vyspělejší v užití ICT a spousta nástrojů vhodných ke kybernetickým útokům je volně šiřitelná v podobě informací, ale také v podobě hotového softwaru a hardwaru, kdy typickým příkladem jsou skimmingové zařízení na bankomaty.

Obrana proti kybernetickým útokům není a nebude ani v budoucnu jednoduchá. Je však nutné investovat do vývoje modernějších a bezpečnějších technologií na obranu kyberprostoru a ochranu uživatelů. K bezpečnějšímu kyberprostoru v budoucnu mohou přispět tři kroky a to poučenější a kompetentnější uživatelé, silná moderní softwarová ochrana (firewally, antiviry a další obranný software) a fyzická ochrana hardwaru (zabezpečení před infikovaným periferním zařízením – kupříkladu USB Disky).

---

[40]DENNING, Dorothy E., Whither cyber terror?, In 10 years after september 11 [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW:, <http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/>

[41] KUŽEL, Stanislav, Kybernetická kriminalita IV: Hacktivismus a kyberterorismus, In BusinessIT [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW:, <http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php>

[42] SIŘINEK, Tomáš, S kyberterorismem jsme se zatím nesetkali. Je to ale otázka času, varuje odborník na bezpečnost, In Avokádo [online]. 28.08.2017, [cit. 2019-06-10]., dostupné na WWW:,<http://avokado-online.cz/s-kyberterorismem-jsme-se-zatim-nesetkali-je-to-ale-otazka-casu-varuje-odbornik-na-bezpecnost/>

ZÁVĚR

Hlavním cílem práce bylo teoretické vymezení základního pojmosloví a východisek zkoumané oblasti kybernetického terorismu. V rámci jednotlivých subkapitol teoretické části práce byl zahrnut i historický exkurs k terorismu, na jehož základě bylo také možné definovat hlavní znaky definující teroristický čin. Je zde dále definován kyberprostor a nástroje užívané v kyberprostoru pro vedení útoků. Rámcové teoretické definování a vymezení základního pojmosloví a východisek je nezbytné pro samotné vymezení pojmosloví kybernetického terorismu, aktérů kybernetického terorismu a jejich nástrojů.

V rámci rámcové analýzy účinné vnitrostátní právní úpravy zkoumané problematiky vyplývá, že v současné době je trend navyšování úrovně bezpečnosti v kybernetickém prostoru, avšak některé legislativní úpravy nedrží krok s vývojem ICT a reakce státu je někdy zpozděna. Pozitivní změnou pro vývoj bezpečnosti ICT bylo přijetí zákona o kybernetické bezpečnosti, kterým Česká republika reagovala na povinnost ratifikovat Úmluvu o kybernetické bezpečnosti a Dodatek k úmluvě o kybernetické bezpečnosti rady EU.

Rámcová analýza mezinárodních právních norem věnujících se kybernetické bezpečnosti ukázala, že jediným významným prvkem mimo výše uvedené Úmluvy o kybernetické bezpečnosti a jejího Dodatku je Tallinnský manuál, který pojednává spíše o kybernetické válce a stanovuje, že každá země je zodpovědná za svůj kybernetický prostor, pro který platí stejná pravidla jako pro fyzický svět. Na poli mezinárodní spolupráce je tak dost veliký prostor pro započetí spolupráce mezi státy a mezinárodními organizacemi v oblasti kybernetické bezpečnosti.

Na vybraných situačních příkladech kybernetických útoků je patrné, že v historii v rámci různých konfliktů probíhaly na pozadí také kybernetické útoky. Pro tyto útoky jsou vyvíjeny stále složitější a účinnější nástroje, které se dají kategorizovat jako kybernetické zbraně. Z odborného pohledu jsou tyto akty pouze kybernetickými útoky, neboť do současné doby nebyl zaznamenám kybernetický útok vedený teroristickou skupinou či hnutím. Teroristé zatím raději volí konvenční prostředky než kybernetické nástroje. Kybernetický terorismus je tak zařazen v rovině teoretické bezpečností hrozby. Tato bezpečnostní hrozba je však reálná a je potřeba s ní

v budoucnu počítat, protože trend vývoje ICT a provázanost fyzického světa s kyberprostorem stále stoupá a ovlivňuje stále více lidí, strojů, zařízení a technologií.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. BRZYBOHATÝ, Marian. *Terorismus I*. Praha: Police History, 1999. 141 s. ISBN 80-9026-70-1-7.
2. BRZYBOHATÝ, Marian. *Terorismus II*. Praha: Police History, 1999. 187 s. ISBN 80-9026-70-4-1.
3. DUNNIGAN, James F. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*. Praha: Baronet, 2004. 356 s. ISBN 80-7214-642-4.
4. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.
5. HROMADA, M. HRŮZA, P. KADERKA, J. LUŇÁČEK, O. NEČAS, M. PTÁČEK, B. SKORUŠA, L. a SLOŽIL, R. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.
6. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. 524 s. ISBN 978-80-88168-15-8.
7. *KOLEKTIV* Autorů, *Terorismus a my: základy sebeobrany*. Praha: Computer Press, 2001. 219 s. ISBN 80-7226-584-9.
8. KOVÁŘ, Milan. *Terorismus III*. Praha: Police History, 2007. s 254. ISBN 978-80-86477-00-8.
9. ŘEHÁK, David, Pavel FOLTIN a Richard STOJAR. *Vybrané aspekty soudobého terorismu*. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2008. 143 s. ISBN 978-80-7278-443-1.
10. SEITZ, Justin. *Python: pro hackery a reverzní inženýrství*. Brno: Zoner Press, Encyklopedie Zoner Press. 2009. 216 s. ISBN 978-80-7413-048-9.
11. *Trestní právo: (soubor zákonů)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, [2018]. ISBN 978-80-7380-707-8.

Online zdroje

1. BRUNE, Štěpán, Hacker může útočit i pomocí chytré televize, říká výzkumník počítačových virů Jiří Gogela, e15.cz [online], 27.03.2019 [citace 2019–04-10], dostupné na WWW: <https://www.e15.cz/rozhovory/hacker-muze-utocit-i-

pomoci-chytre-televize-rika-vyzkumnik-pocitacovych-viru-jiri-gogela-1357483>

2. BRZYBOHATÝ, M. Současný terorismus. Vojenské rozhledy. Praha, 2002, roč. 11 (43), č. 2, s. 46—62. ISSN 1210-3292.
3. Definition by Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, In Draft Pisa . [online]. [cit. 2019–04-01], dostupné na WWW: <https://www.academia.edu/7096442/How_would_you_define_Cyberspace>
4. DENNING, Dorothy E., Whither cyber terror?, *In 10 years after september 11* [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW:, <http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/>
5. DRMOLA, Jakub, Konceptualizace kyberterorismu, Vojenské rozhledy, [online]. 2013, roč. 22 (54), č. 2, s. 94–102 [cit. 2019-05-10], ISSN 1210-3292. Dostupné z WWW: <http://vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu>.
6. ERBEN, Lukáš, Příchod hackerů: Příběh Stuxnetu, In root.cz [online]. 29.04.2014, [cit. 2019-06-10]., dostupné na WWW: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>
7. FLÍDR, Tomáš, Mezinárodní právo v kyberprotoru a Tallinský manuál, *In Kyberbezpečnost,* 22.11.2013 [online]. 22.11.2013, [cit. 2019-07-01]. dostupné na WWW: <https://www.kyberbezpecnost.cz/?p=198>
8. FOLTIN, Pavel, ŘEHÁK, David, Historický vývoj terorismu, In Obrana a strategie [online]. 09.07.2007, [cit. 2019-05-10]. Dostupné z WWW: <https://www.obranaastrategie.cz/filemanager/files/6263.pdf>
9. "I DON'T EVEN HAVE A MODEM", interview Jan Josefsson, 1995. [online]. [cit. 2019–04-30], dostupné na:< http://www.josefsson.net/gibson/index.html>
10. GovCert.cz, Národní centrum kybernetické bezpečnosti [online], [cit. 2019-06-25], dostupné na WWW: <https://www.govcert.cz/cs/vladni-cert/govcert-cz/>
11. JANOUŠEK, Michal, Kyberterorismus: Terorismus informační společnosti, In Obrana a strategie [online]. 20.03.2007, [cit. 2019-05-10]. Dostupné z WWW: <https://www.obranaastrategie.cz/filemanager/files/6513.pdf>
12. KUŽEL, Stanislav, Kybernetická kriminalita IV: Hacktivismus a kyberterorismus, In BusinessIT [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW:, <http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php>

13. KUŽEL, S. Kybernetická kriminalita od hackerů ke kybernetickým válkám. In Business It. [online]. [cit. 2019–04-30]. Dostupné z WWW: <http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php>
14. PAVLÍKOVÁ, Miroslava, Estonsko-ruský incident v kontextu kyberterorismu, Global Politics [online]. 19.01.2014, [cit. 2019-06-10]., dostupné na WWW: <http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu>
15. Rok 2019 bude ve znamení sofistikovanějších bezpečnostních útoků, SecurityWorld [online], 26.12.2018, [cit. 2019-05-10], dostupné na WWW: <https://computerworld.cz/securityworld/rok-2019-bude-ve-znameni-sofistikovanejsich-bezpecnostnich-utoku-55111>
16. SIŘINEK, Tomáš, S kyberterorismem jsme se zatím nesetkali. Je to ale otázka času, varuje odborník na bezpečnost, In Avokádo [online]. 28.08.2017, [cit. 2019-06-10]., dostupné na WWW:,<http://avokado-online.cz/s-kyberterorismem-jsme-se-zatim-nesetkali-je-to-ale-otazka-casu-varuje-odbornik-na-bezpecnost/>

Legislativní dokumenty

1. ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z WWW: <https://www.zakonyprolidi.cz/cs/2014-181#redakce>
2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 394 - 406. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40 >
3. ČESKO. Zákon č. 141/1961 Sb., trestní řád. In Sbírka zákonů, Československá socialistická republika. 1961, částka 66, s. 513 - 576. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1961-141#cast2 >

SEZNAM ZKRATEK

ČR – Česká republika

ES – Evropské společenství

EU – Evropská unie

ICT – Informační a komunikační technologie

IOT – internet věcí

TŘ – zákon č. 141/1961 Sb. trestní řád, ve znění pozdějších předpisů

TZ – zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

ZKB – zákon o kybernetické bezpečnosti

SEZNAM TABULEK A GRAFŮ