POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Vigilantismus v kyberprostoru

Bakalářská práce

Vigilance in cyberspace

Bachelor thesis

VEDOUCÍ PRÁCE

doc. PhDr. Marian BRZYBOHATÝ, Ph.D.

AUTOR PRÁCE

Jan WOLF

PRAHA

2023

Čestné prohlášení

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

V Mělníku dne 26.2.2023

Jan Wolf

ANOTACE

Tato bakalářská práce se zabývá tématem vigilantismu v kyberprostoru. Skupiny či jednotlivci v tomto případě tzv. „vigilantisté“ využívající moderní způsoby, které jim nabízí dnešní doba, především síť Internet, kyberprostor, a mobilní zařízení umožňující se připojit do onoho virtuálního světa. Často suplují orgány činné v trestním řízení, vypátrávají a trestají osoby, které se v jejích očích něčím provinily a mnohdy se tak sami dopouštějí protiprávního jednání. V teoretické části dochází k vymezení pojmu vigilantismu a s ním souvisejících termínů, k představení některých vigilantistických subjektů a k popsání nejpoužívanějších metod. V praktické části pak jsou zhodnoceny dopady a rizika na základě vybraných případů, které se v minulosti ve světe nebo v České republice odehrály.

KLÍČOVÁ SLOVA

Vigilantismus, kybervigilantismus, digilantismus, online vigilantismus, kyberprostor, hacktivismus, DDoS útok, Anonymous

ANNOTATION

This bachelor thesis deals with the topic of vigilantism in cyberspace. Groups or individuals, in this case so-called "vigilantes", using the modern ways offered by today's times, especially the Internet, cyberspace, and mobile devices that allow them to connect to that virtual world. They often substitute for law enforcement authorities, tracking down and punishing people who, in their eyes, are guilty of something, often committing illegal acts themselves. In the theoretical part, the concept of vigilantism and related terms are defined, some vigilante subjects are introduced and the most used methods are described. The practical part then assesses the impacts and risks based on selected cases that have occurred in the past in the world or in the Czech Republic

KEYWORDS

Vigilantism, cybervigilantism, digilantism, online vigilantism, cyberspace, hacktivism, DDos attack, Anonymous

OBSAH

ÚVOD

Vigilantismus má v historii lidstva své nezaměnitelné místo, v některých lidech je zakořeněná potřeba brát spravedlnost do vlastních rukou a potrestat hříšníka. V životě se jistě každý s určitou formou nespravedlnosti setkal. Jak se ovšem proměnil vigilantismus s příchodem moderních technologií a internetu a jaké možnosti nabízí vigilantistům právě internet, sociální sítě, moderní technologie, to je tématem této práce.

Žijeme v době, ve které se informační technologie rozvíjejí každým rokem rychleji a rychleji, v době, kdy se spousta věci digitalizuje, analogová podoba se převádí do té digitální a je tak čitelná za použití výpočetních zařízení. Výrobci těchto zařízení nás každý rok oslňují novými produkty, které jsou v porovnání s těmi loňskými daleko modernější, rychlejší, vybavenější, odolnější atp. a ono tomu skutečně tak je. Ani pandemie virového onemocnění, se kterou se lidstvo v posledních letech potýkalo, tento pokrok nezastavila, možná jej pouze zbrzdila, a to pouze v tom směru, že je nedostatek výrobních součástek. Lidé marně čekající na vyřízení předobjednávky nového telefonu už pomalu vyhlíží příchod jeho nástupce, tak rychlý je dnešní pokrok. A to nejen co se samotných počítačových zařízení týká, ruku v ruce s tím jde i neustálý vývoj softwaru, operačních systému, všemožných programů, aplikací a samozřejmě internetu a kyberprostoru. Stejně tak, jak se modernizuje náš reálný svět, modernizuje se i ten virtuální. Do virtuálního světa se přesouvají nejen digitalizované dokumenty, ale spoustu dalšího. Informace, osobní údaje, zábava, studium, zaměstnání, sociální aktivity, ale také například boje, kriminalita, to vše se zdigitalizovalo. S trochou nadsázky lze říct, že ve virtuálním světe se dá žít i prožívat život velice podobně, ne-li stejně jako ve světě reálném. V kyberprostoru nalézáme přátelé, své protějšky, své nepřátelé, komunikujeme s úřady, podáváme daňová přiznání, díky tomuto světu prožíváme spoustu emocí, stáváme se závislými na moderních technologiích a kyberprostoru.

I vigilantismus se modernizoval a jeho část se přesunula do digitálního prostoru, kde se zákonitě musel přizpůsobit podmínkám kyberprostoru. První část této práce si klade za cíl vymezit samotný pojem vigilantismu a jeho proměnu při přechodu do kyberprostoru. Budou přiblíženy a popsány některé metody vigilantistů v kyberprostoru a dále také představeny vybrané skupiny či jednotlivci,

kteří, ač si to možná neuvědomují, vigilantisty v kyberprostoru jsou či si tak počínají. V druhé, praktické části, pak dojde k vyhledání konkrétních příkladů vigilantismu v kyberprostoru, jejich krátkému vylíčení a následnému zhodnocení dopadů a rizik pro dotčené osoby.

1. TEORETICKÁ ČÁST

1.1 Internet

Pro pochopení následujících pojmů, zejména pak pojmu kyberprostor, je vhodné nejprve vymezit pojem *internet.* Jedná se o složeninu slov *interconnected* a networks, tedy v češtině *vzájemně propojené sítě*. „*Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem*.“ [1]

Internet se stal součástí našich životů a těžko si lze představit pokračování běžného života bez něho. Pomocí připojení do Internetové sítě konzumujeme informace, jsme v kontaktu s přáteli, pracujeme, bavíme se, učíme se, řídíme chytré domácnosti, provádíme nespočet činností. Jako samozřejmost se dnes pokládá připojení k internetu pomocí mobilního telefonu, notebooku, počítače, tabletu, ale k internetu jsou dnes připojeny i různé domácí spotřebiče, televize, lednice, pračky, kávovary, termostatické hlavice radiátorů, osvětlení, ani vozidla a hračky pro děti nejsou výjimkou, takřka jakékoli elektronická zařízení schopná provádět jednoduché nebo složitější operace lze připojit k internetu.

Podle Českého statistického úřadu má v současnosti v České republice 85 % domácností přístup k internetu a počítač (stolní počítač, notebook, tablet) má 81 % domácností. Pro srovnání před dvanácti lety mělo přístup do sítě Internet jen 56 % domácností a počítač (stolní, notebook nebo tablet) mělo 59 % domácností. [2]
Mobilní telefon, který je dnes běžně připojen do sítě Internet, měl v roce 2021 v České republice, až na výjimky, každý člověk starší 16 let a z toho tři čtvrtiny využívaly mobilní Internet. [3] Je tedy víc než zřejmé, že mladá generace lidí je

[1] KOLOUCH, Jan. *Cybercrime.* 1. Praha: CZ.NIC, 2016, s. 43. ISBN *978-80-88168-18-8*
[2] ČESKÝ STATISTICKÝ ÚŘAD [ČSÚ]. *Počítače a internet v domácnostech. In: Český statistický úřad* [online]. Praha, *2022 [cit. 1.12.2022]* dostupné z: https://www.czso.cz/documents/10180/164606768/0620042201.pdf/5699654d-a722-44c9-a5e8-80443c89be18?version=1.1
[3] ČESKÝ STATISTICKÝ ÚŘAD [ČSÚ]. *Internet zrychluje a přesouvá se na chytré telefony*, In: *Český statistický úřad* [online]. Praha, *2022, [cit. 1.12.2022,]* dostupné z: https://www.czso.cz/csu/czso/internet-zrychluje-a-presouva-se-na-chytre-telefony

digitálně gramotná a jejich životy jsou a s největší pravděpodobností budou internetem protkané.

Internet je neodmyslitelnou součástí života nejen v České republice. Bezpochyby je internet velká „věc“, která ovšem není věcí z pohledu českého práva. Občanský zákoník v § 489 nazývá věc vším, *co je rozdílné od osoby a slouží potřebě lidí*. [4] Dále by se dle § 496 odst. 1 dalo říct, že internet je hmotná věc, jelikož ta je zde definována jako „*ovladatelná část vnějšího světa, která má povahu samostatného předmětu“.* [4]

Je zcela evidentní, že internet není osobou (fyzickou ani právnickou) a zároveň zcela výrazným způsobem lidem slouží, mohlo by se tedy zdát, že se skutečně jedná o věc dle občanského zákoníku, a právě o věc hmotnou. K této záležitosti se vyslovil i V. Smejkal v knize Kybernetická kriminalita, kde popisuje důležité rysy věci, a to možnost jí vlastnit a ovládat, doslova říká: *„Internet jako celek si nelze přivlastnit, ani jej ovládat. Internet není věcí v právním slova smyslu.“* [5] Vlastněny mohou být pouze části internetu, jako jsou počítačové sítě a poskytované služby.[6]

1.2 Kyberprostor

Pokud víme, že internet je celosvětová počítačová síť složená z menších sítí, co je pak kyberprostor. Rozhodně se nejedná o synonymum, i když laická veřejnost leckdy tyto pojmy zaměňuje. V zákoně č. 181/2014 Sb., o kybernetické bezpečnosti je pojem kyberprostor (kybernetický prostor) definován jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*.[7]

V románu Neuromancer, Wiliam Gibson formuloval *kyberprostor* slovy:

„*Sdílená halucinace každý den pociťovaná miliardami oprávněných operátorů všech národů, dětmi, které se učí základům matematiky… Grafická reprezentace*

[4] Zákon č. 89/2012 Sb., Zákon občanský zákoník. In: *Zákony pro lidi* [online]. © AION CS, 2010-2023 [cit. 2.12.2022]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2012-89

[5] SMEJKAL, Vladimír. *Kybernetická kriminalita.* 1. Plzeň: Aleš Čeněk, 2015, s. 60. ISBN 978-80-7380-502-2

[6] KOLOUCH, Jan. *Cybercrime.* 1. Praha: CZ.NIC, 2016, s. 92. ISBN *978-80-88168-18-8*

[7] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Zákony pro lidi* [online]. © AION CS, 2010-2022 [cit. 2.12.2022]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2014-181

dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, ustupující…"[8] Poprvé tento pojem použil v krátké povídce s názvem Burning Chrome v roce 1981, ale až v románu Neuromancer jej definoval. Sám Gibson v pozdějších letech tento pojem zpochybňoval, když jej použil, zdál se mu módní a efektivní, ale také mu připadal sugestivní a v podstatě nesmyslný, přesto se pojem kyberprostor v dnešní době hojně užívá a vzniklo a stále vzniká nespočet pojmů s předponou *kyber*, které jsou dnes zažité a určují právě to, že se nějakým způsobem týkají virtuálního světa – kyberprostoru. Může jít o relativně nově vzniklé hrozby – kyberhrozby jako kyberšikana, kyberkonflikt, kyberterorismus. Nebo naopak pojem bezpečnost ve virtuálním světe, tedy kyberbezpečnost, ale může jít i o pojmy spojené s chorobným strachem z počítačů, virtuální reality a jejího rozvoje zvaný kyberfobie. Žádný z těchto pojmů by jistě nevznikl nebýt toho prvního použitého výrazu kyberprostor.

„*Kyberprostor je virtuální realitou, nemající konce ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světe reálném."*[9] Takto stručněji a možná i uchopitelněji formuloval pojem J. Kolouch v knize CyberSecurity, jedná se o čerstvější pohled na termín. Osobně bych kyberprostor nenazýval virtuální realitou, stejně tak jako kyberprostor není internet, není ani virtuální realitou. Tu bych chápal spíše jako simulované prostředí, jakousi podmnožinu kyberprostoru. K oné Kolouchově definici bych doplnil ještě, že tento prostor je závislý také na všech osobách, fyzických a právnických, které do něho vstupují a přímo jej ovlivňují.

I osoba, která v kyberprostoru zdánlivě nic nedělá, např. jen konzumuje obsah vytvořený jinými, se podílí na fungování tohoto virtuálního světa a ovlivňuje jej, třebaže nepřímo.

Kyberprostor už možná není jen jakýsi virtuální svět, ale vesmír neustále se rozpínající a oproti vesmíru i čím dál tím bohatší, čím více zařízení a služeb do něho vstupuje, tím ten pomyslný vesmír narůstá.

---

[8] Gibson, William. *Neuromancer*, Plzeň: Laser – books, 1998, s. 54. ISBN 80-7193-048-2

[9] KOLOUCH, Jan, BAŠTA, Pavel, KROPÁČOVÁ, Andrea, KUNC, Martin. *CyberSecurity.* 1. Praha: CZ.NIC, 2019, s. 36. ISBN 978-80-88168-34-8

1.3 Vigilantismus

V anglickém jazyce běžně používaný termín *vigilante*, kterým můžeme označit drtivou většinu superhrdinů v komiksech o Batmanovi, Spidermanovi, Supermanovi atp. (typickým příkladem vigilantisty mnohokrát zfilmovaným je postava Robina Hooda), v českém jazyce bychom jednoslovný (případně výstižný víceslovný) překlad tohoto slova těžko nalezli, nepřekládá se nebo je nahrazen jiným vhodným slovem zapadajícím do kontextu. Jednoznačná a celistvá definice tohoto pojmu neexistuje. Velmi jednoduše řečeno, vigilantisté jsou lidé beroucí zákon do svých rukou. Ovšem v této práci se jedná o zcela zásadní pojem, který je nutné formulovat podrobněji. Slovo vigilant má původ v latině a znamená bdělý nebo ostražitý. O jedno z prvních vymezení pojmu se pokusil Les Johnston ve dvouměsíčníku zaměřeném pro britskou a mezinárodní kriminologii a právo Brithish Journal of Criminology na jaře 1996, zde uveřejnil článek, ve kterém určil šest nezbytných znaků vigilantismu:

1. Jedná se o plánovanou a promyšlenou činnost.
2. Účastníci jsou soukromé osoby, které se do činnosti zapojují dobrovolně.
3. Jedná se formou "autonomního občanství" a jako takový představuje sociální hnutí.
4. Používá sílu nebo jejím užitím hrozí.
5. Vzniká v případech, ve kterých došlo k ohrožení či potenciálnímu překročení či přímému překročení zákonných norem.
6. Cílem je kontrola kriminality nebo jiných společensky škodlivých jevů a zajistit bezpečnost sobě a ostatním.[10]

Ze znaků, které představil Johnston se dá dovodit, že vigilantismus není bezprostředním aktem, i když se může jednat o rychlou reakci na porušení morálních nebo zákonných norem (i těch, které si vigilantisté subjektivně vykládají), je formou koordinovaného jednání. Zapojují se do něho pouze civilisté, není to jednání orgánů státní moci. Důležitým prvkem je použití síly nebo hrozba použití síly, jejíž důsledky je nutné chápat jako jakoukoli újmu jiné osobě, zejména

[10] JOHNSTON, Les. What is vigilantism?, In: *Oxford University Press*, [online]. Velká Británie, 1996 [cit. 3.12.2022]. Dostupné z: https://doi.org/10.1093/oxfordjournals.bjc.a014083

pak se může jednat o formu fyzického násilí – tedy újmu na zdraví či hrozbu újmy na zdraví. Vytváří se především tam, kde může být pociťována určitá forma nespravedlnosti, morálního rozhořčení, lhostejnosti, nedostatečně vysokého trestu nebo dokonce jeho absence, tam kde je právo přehlíženo, v případech, kde není postupováno zcela adekvátně, rychle, rázně. Cílem bývá nejen ochrana morálních a zákonných norem, ale i satisfakce, potrestání viníka.

Velice výstižně pojem shrnul J. Drmola: „*Vigilantisé jsou lidé, kteří vynucují dodržování státních zákonů a společenských norem (resp. dodržování jejich vlastní interpretace těchto zákonů a norem, a přitom nejsou součástí jakékoliv státní instituce či složky tímto se zabývající a postrádají jakoukoliv oficiální autoritu.“*[11]

1.3.1 ***Kybervigilantismus***

Jak bylo nastíněno v úvodu, s neustálým vývojem technologií a internetu se nutně musel vyvinou i vigilantismus. Ne, že by jeho původní konvenční verze zanikla, to vůbec ne, jen se jeho část přesunula právě do kyberprostoru, digitalizovala se. Taková forma vigilantismu pak bývá označována jako vigilantismus v kyberprostoru, kybervigilantismus, digitální vigilantismus neboli digilantismus, či někdy netilantismus. S přenosem vigilantismu do kyberprostoru vznikají pro vigilantisty zcela nové možnosti, které jim poskytuje síť Internet.

Ačkoli by se mohlo zdát, že kybervigilantismus je jen vigilantismem v kyberprostoru a Johnstonova teorie by se rozšířila o sedmý znak, který by mohl vypovídat o tom, že jednání probíhá v kyberprostoru nebo za využití sítě Internet a jeho služeb, není to mu úplně tak. Přeci jen digitální prostor není to samé, co reálný svět, ať svým způsobem jsou si oba světy/prostory podobné. Daniel Trottier o digilantismu ve své práci s názvem „Digital Vigilantism ad Weaponisation of Visibility“ napsal: *„Digitání vigilantismus je proces, ve kterém jsou občané kolektivně pohoršeni aktivitou jiných občanů a reagují koordinací odvetných*

[11] DRMOLA, Jakub. *Protidžihádský vigilantismus v kyberprostoru.* 1. *Brno: EDIS, 2018, s. 60 ISBN: 978-80-210-8985-3*

opatření na mobilních zařízeních a sociálních platformách"[12]*.* Dále Trottier rozšiřuje a upravuje Johnstonovy znaky v případě digilantismu.

1. bod plánování a promyšlenost zůstává. Aby se jednalo o kybervigilantismus, je i v tomto případě potřeba určitá míra plánování a promyšlenosti, ale v případě kybervigilantismu je značně usnadněna spontánní spolupráce a překážky materiální, časové a prostorové zcela odpadají.

2. bod sdělující nám, že jednají vždy civilní osoby nikoli např. policejní složky, Trottier rozšiřuje a říká, že vztah s policií může být komplikovaný. I zde jsou kybervigilantisté civilní osoby, ovšem někdy právě policie může vyvolat jejich reakci, a to zejména v případech, ve kterých se policie v nějakém konkrétním případě obrací s žádostí o pomoc právě na obyvatelstvo. Jako příklad může posloužit nedávný incident (napadení osob pravděpodobně pro jejich sexuální orientaci) ze stanice metra Kobylisy z 20.12.2022, ve kterém policie pátrá po osobě muže v modré bundě, který je zachycen na videozáznamu. I taková stručná prosba k veřejnosti může být příčinou jednání vigilantistů v kyberprostoru.

3. bod a pojem „autonomního občanství" chápe jako sebeobranu jednotlivců či skupin v rámci daného konkrétního území. Kyberprostor ve své podstatě žádné hranice nemá, a tak je i tento bod komplikovaný, ale ne nutně vyloučeným.

4. bod použití síly nebo hrozba použití síly s příchodem kybervigilantismu může přispívat k fyzickému násilí, velké zastoupení má zde spíše kulturní násilí a zviditelňování cílů. Jako zbraň zde slouží právě zviditelnění (tedy podle Trottiera tzv. „weaponized visibility"), která je samozřejmě pro zasaženou osobu nebo osoby nežádoucí. Jednoduše lze sdělit, že klasické fyzické násilí se přeměňuje v digitální útoky různého typu, následkem pak jsou např. ztráta soukromí, finanční újma, veřejné ponížení.

5. bod je opět komplikovaný a dá se říci, že přímo navazuje na bod 3. teritorium. V každé zemi panují určité odlišnosti v otázkách práva a pohledu na to, co morální je a co není. Kybervigilantismus v tomto bodě je jakýmsi propojením informací s obecnými normami v digitálním světě.

[12] TROTTIER, Daniel. Digital Vigilantism as Weaponisation of Visibility, In: *Springer Nature Switzerland* [online]. Švýcarsko, 2017 [cit. 4.12.2022], Dostupné z: https://link.springer.com/article/10.1007/s13347-016-0216-4

6. bod definující bezpečnost osobní a kolektivní, který jistě platí i v případě kybervigilantismu, ale je spíše chápán opět na nějaké lokální úrovni, s nějakými hranicemi, vyvstává zde otázka hranic kyberkolektivu.

„Kybervigilantismus sice využívá výlučně prostředí a nástrojů kyberprostoru, ale může takto napadat cíle a aktivity mimo něj.“[13]

1.4 Nejčastěji používané nástroje digilantistů

Cílem této kapitoly není kompletní výčet všech metod využívaných digilantisty, ale seznámit s těmi pravděpodobně nejpoužívanějším a možná i méně známými. Níže uvedené popsané metody nevyužívají pouze vigilantisté v kyberprostoru, ale jsou to funkční nástroje, které využívají i jiní útočníci k dosažení svých cílů, osoby páchající trestnou činnost, crackeři. Osoba zvaná cracker je počítačově zdatný jedinec znalý velice dobře hardware, software a jeho tvorbu. Jedná se hackera řadícího se do skupiny „Black hat Hacker“ do českého jazyka se význam nepřekládá, ale název je odvozen od barvy klobouku (černá symbolizuje něco špatného, bílá něco dobrého, šedá barva něco mezi tím). Jedná se tedy o hackera, který své znalosti využívá ve svůj vlastní prospěch s cílem se obohatit, případě způsobit druhému škodu. Opakem Black Hat Hackera je White hat (tzv. etický hacker), případně přímo specialista na bezpečnost, ten velice jednoduše řečeno se snaží díky svým znalostem „pomáhat“, poukazuje na zranitelnost programů, služeb atp. Gray hat je pak hacker, který může porušovat některé morální hodnoty, případně i zákonné normy, ovšem nemá přímo zlé úmysly jako Black hat, pohybuje se v tzv. šedé zóně mezi dvěma zmíněnými extrémy.

Není vyloučeno, že hacker nemůže být zároveň vigilantistou, naopak, díky svým nadprůměrným znalostem informačních technologií by byl takový člověk velmi efektivním v řadě útoků či vyhledávání informací.

1.4.1 Doxing

Doxing, psán také jako doxxing či d0xing. Pojem je zkráceným výrazem slovního spojení „Droping dox“. „Dox“ je moderní slangový výraz anglického slova documents (dokumenty) resp. jeho zkrácenou formou „doks“, v češtině termín

[13] DRMOLA, Jakub. *Protidžihádský vigilantismus v kyberprostoru.* 1. *Brno: EDIS, 2018, s. 62, ISBN: 978-80-210-8985-3*

znamená něco jako zveřejnění souborů. Jedná se o metodu vyhledávání a následného zveřejňování osobních údajů lidí bez jejich souhlasu. Předmětem zveřejnění může být jméno, příjmení, datum narození, fotografie uživatele, e-mail, tel. číslo, bydliště, číslo osobního dokladu, zkrátka jakýkoli osobní údaj nebo údaje osoby, které mohou vést k její identifikaci. Doxeři (doxxeři), lidé, kteří odhalují identitu druhého, čerpají v kyberprostoru různé informace např. na sociálních sítích, využívají otevřených zdrojů, volně dostupných informačních kanálů v síti Internet, ale také např. z uniklých databází různých společností nacházejících se pro běžného uživatele internetu na nedostupných místech. Prakticky kdokoli se dá vysledovat na internetu, každý po sobě nějakou digitální stopu zanechá, spousta lidí na sociálních sítích ochotně sdílí své osobní údaje, fotografie, příběhy ze svého každodenního života, místo, kde žije, nebo dokonce označuje přesnou polohu, kde se zrovna nachází on sám nebo se svými přáteli a známými. Mnoho lidí používá shodná uživatelská jména napříč sociálními sítěmi, což usnadňuje doxerům pátrání po osobních informacích. Samotné získávání informací o jedinci nebezpečné není, to ale cílem doxingu není. Cílem je naopak vystavit osobu velmi nepříjemní situaci, zveřejněním informací narušit její soukromí, zostudit ji, zesměšnit, ponížit nebo zastrašit či se prostě jen pomstít.

Následek pro oběť doxingu může být relativně neškodný, prosté zveřejnění nějaké informace až po vcelku zásadní zásah do jejích práv, mnohdy zasahující i rodinné příslušníky, přátelé či rodinu.

1.4.2 ***DoS, DDoS***

Dvě zkratky jejichž anglický význam zní „Denial of Service“ a „Distributed Denial os Service“, do českého jazyka lze přeložit jako „odepření služby“ a „distribuované odepření služby“. Jak již název napovídá, cílem této metody je znepřístupnit, omezit fungování či úplně vyřadit z provozu nějakou službu, běžně například webovou stránku. „*Tento útok je realizován zahlcením napadeného počítačového systému (či prvku sítě) pomocí opakujících se požadavků na úkony, které má počítačový systém vykonat. Tento útok může být realizován i zahlcením informačních kanálů mezi serverem a počítačem uživatele či zahlcením volných systémových prostředků. Systém napadený DoS útokem se projevuje zejména*

neobvyklým zpomalením služby, celkovou nebo chvilkovou nedostupností služby (např. webových stránek) apod.“[14]

Rozdíl mezi službou DoS a DDoS spočívá pouze v tom, z kolika zařízení je útok prováděn. V případě DoS útoku se jedná vždy o jedno zařízení. Jedná se o jednodušší typ útoku, který je také možné i jednoduše eliminovat. V případě DDoS útoku přichází na cílové zařízení více útoků současně z různých zařízení umístěných v různých lokalitách, je rozložen do několika dílčích útoků, které probíhají současně. Proti takovému typu útoku je mnohem těžší se bránit. Útoky mohou pocházet ze zařízení velkého množství útočníků (kybervigilantistů) nebo z tzv. botnetů (síť infikovaných výpočetních zařízení/počítačů malwarem – škodlivým kódem, ovládaná jedním útočníkem, bez vědomí majitele či uživatele onoho zařízení).

Cílem obou útoků není překonání bezpečnostního opatření zařízení, na které je útočeno a proniknout tak do něho či získat jakákoli data, cílem je pouze zatížit hardware natolik, aby zařízení (služba) v ideálním případě bylo nedostupné, vyřazené z provozu nebo alespoň, aby fungovalo s obtížemi, bylo zahlceno a nebylo schopno vyřizovat legitimní požadavky jiných uživatelů. Výsledkem takového útoku může být nedostupný web nebo v případě dostupnosti pomalá či problémová odezva webu (nebo poskytované internetové služby).

1.4.3 ***Scambaiting***

Jedním z naprosto příkladnou metodou využívanou právě digilantisty je scambaiting, slovo nemající český ekvivalent podobně jako v případě slova vigilantismus, prozatím se nepřekládá. Jedná se o složeninu dvou anglických slov „bait“ a „scam“, „návnada“ a „podvod“. Je to aktivita v kyberprostoru, kterou jsou podváděni internetoví podvodníci. Člověk, který loví podvodníky na internetu, si říká nebo je ostatními nazýván jako scambaiter využívá stejné nebo podobné techniky jako podvodník na kterého útočí, tzv. ho přechytračí.

Scambaiting mimo jiné využívá techniku zvanou „sociální inženýrství“. Není to forma útoku jako ve výše popsaných případech, ale dá se přirovnat k manipulaci s lidmi, je to určitá sociální dovednost komunikace člověka přesvědčujícího či

[14] KOLOUCH, Jan. *Cybercrime.* 1. Praha: CZ.NIC, 2016, s. 295-296. ISBN *978-80-88168-18-8*

získávajícího užitečné informace. Získaná informace, služba nebo přístup do nějakého systému se následně dají použít k nějakému útoku. Může se jednat o prostý telefonát oběti, při kterém se dotyčný představí jako nadřízená autorita požadující určité informace nebo např. podvodným e-mailem požadujícím přihlašovací údaje do internetového bankovnictví – tzv, phishing.
Scambaitři reagují právě na podvodné e-maily, nabídky (např. podvodné investice do kryptoměn) nebo prodeje zboží a lákají ze svých obětí (podvodníků) cenné informace, zdržují je od jejich „práce“ a často si i své počínaní zaznamenávají a šíří je na sociálních sítích.
Cílem scambaitingu je zabránění podvodníkovi v jeho aktivitách, odhalit jeho totožnost, zesměšnit ho (doxing), získat jakékoli relevantní informace, které mohou pomoci jeho obětem. V současnosti je nejznámějším scambaiterem americký streamer vystupující pod aliasem Kitboga, působí na platformě Youtube, Twitter a Twitch, zmínit mohu další známé skupiny či osoby jako např. Scambaiter, Scammer Payback, ScammerRevolts, Jim Browning.

*1.4.4 **Hacktivism***

Opět se jedná slovní spojení dvou anglických slov „hacking“ a „activism“, často také nazýván Internetový aktivismus. Hacktivismus je hackerská činnost motivovaná občanskými, politickými nebo náboženskými důvody. Hacktivista je pak osoba, která aktivně zapojuje do hacktivismu.
Ze samotného názvu vyplývá, že k politicky či občansky motivovaným cílům jsou používány hackerské metody – násilného případně skrytého vnikání do počítačových systémů, šířením škodlivého softwaru, vytváření různých webů nebo nežádoucí úprava, jíž existujících webových stránek atd. Formou útoků v kyberprostoru je usilováno o nějakou společenskou změnu nebo šíření nějaké zprávy a upozornit tak širší veřejnost na nějakou palčivou záležitost.
Při hacktivismu jsou již využívány znalosti počítačových programů a systémů. Metody využívané při hacktivismu:

- Jednou z podpůrných a hojně využívaných metod jsou *DoS a DDoS útoky* (viz 1.4.2) – v případě hacktivismu slouží zejména k tomu, aby cílovou službu vyřadili z provozu a zabránili tak uživatelům k přístupu k ní.

- *Doxing* (viz 1.4.1) – vyhledávání a zveřejňování citlivých informací o jednotlivci či skupině.
- *Blogování* – velmi oblíbená činnost whistblowerů nebo novinářů. Whistblower v doslovném překladu znamená „ten kdo píská na píšťalku“. V tomto případě tedy na sebe strhává pozornost a informuje o nějakém zásadním problému. Většinou se jedná o bývalé zaměstnance společností, kteří upozorňují na nemorální, neetické či přímo nezákonné počínání svého bývalého zaměstnavatele. Blogováním pak tito lidé předávají informace veřejnosti a zároveň se snaží udržet si anonymitu, převážně se jedná o tzv. anonymní blogování.
- *Poškozování webových stránek* – neoprávněný přístup a změna obsahu na stránkách ve prospěch hacktivistů. Může se jednat o nenápadnou činnost, pozměnění textu ve svůj prospěch, aniž je veřejností a uživatelem webu na první pohled rozpoznána anebo na první pohled patrná úprava stránky. Běžně jde o náhradu obsahu, zveřejnění videa, textu, vulgárních zpráv, zesměšnění uživatele (majitele) stránek.
- *Geobombing* – je technika, kterou hacktivisté lokalizují videa z YouTube v aplikaci Google Earth a Google Maps. Uživatel sdílející video na YouTube má možnost jednoduchým způsobem opatřit video štítkem udávající zeměpisnou polohu. V mapových aplikacích spol. Google lze pak nalézt konkrétní místo, kde bylo video pořízeno, resp. jaká je k němu uvedená zeměpisná poloha. Dříve velmi využívaná technika zejména k zobrazení polohy politických vězňů.
- *Zrcadlení webových stránek* – je technika, kterou je zkopírována celá webová stránka (běžně se jedná o cenzurovaný web) a umístěna na jinou doménu samozřejmě již bez cenzury.
- *Přesměrování webové stránky* – technika, kterou útočník přesměruje uživatele na stránku se svým vlastním obsahem. Uživatel internetu se tak dostane na zcela jiné webové stránky, než zamýšlel.

Využívaných technik v případě hacktivismu může být samozřejmě více a s tím, jak se vyvíjí kyberprostor a technologie obecně možností vigilantistům přibude, a to nejen v případě hacktivismu. Popsané techniky mají posloužit spíše pro

představu, co si pod termínem představit a s jakými dalšími metodami je hacktivismus vázán.

Cíle hacktivismu jsou více než jasné, jedná se o formu protestu v digitální podobě, obcházení cenzury, zveřejňování informací, které mají být utajeny, jedná se o různé druhy podpory a pomoci osobám politicky nebo nábožensky utlačovaným. Je to jednání podporující svobodu projevu zejména v kyberprostoru, brání zájmy společnosti, ale například je jeho snahou i zastavit financování terorismu, podpora demokracie. To vše v subjektivním pojetí samotných útočníků – vigilantistů v kyberprostoru.

1.4.5 ***Human flash search***

Metoda velmi podobná doxingu. Jako první byla použita v Číně v průběhu roku 2000, někdy nazývána i jako Human flash search engine. Původní název byl čínský *„renrou sousou yinqing“* a později přeložen do angličtiny. Oproti doxingu, který stojí na čistém vyhledávání a zveřejňování informací, tato metoda v sobě nese vždy nějaký příběh a v lidech vzbuzuje výrazné emoce. Pokud by se dala k něčemu přirovnat byl by to „hon na čarodějnice“, jen v dnešní době by se jednalo o digitální hon na čarodějnice. Honem na čarodějnice právě proto, že už na základě prvních informací, které se můžou objevit na internetu, sociálních sítích, většinou se jedná o nějaké video (fotografii) vzbuzující v lidech pohoršení (př. týrání zvířete), se plní diskuzní fóra a komentáře pod příspěvky s cílem „pátrání po lidském těle“, odtud název metody. Pohoršení a emoce nemusí být vyvoláno vždy, ale vždy se jedná o velký zájem lidí ke konkrétnímu tématu (např. i k vyvrácení nějakého tvrzení). Zájmový příspěvek nebo video se pak velice rychle šíří na sociálních sítích a mezi jednotlivými uživateli a začíná ono pátrání, které spočívá ve vyhledávání jakýchkoli informací, které by vedly ke ztotožnění osoby (či k jinému cíli).

Oproti doxingu, kde se také vyhledávají a zveřejňují osobní informace je metoda Human flash search odlišná zejména v tom, že se do ní zapojuje obrovské množství lidí, kteří ani nemusejí mít větší počítačové znalosti, jedná se jen o rozhořčené uživatele internetu, nazývají se netizens (velice aktivní jedinci na diskuzních fórech, jedná se pojem složený ze dvou slov „net“ (internet) a „citizen“ (občan), slovní spojení možné chápat jako „uživatel internetu“).

V případě této metody se nabízí určitá paralela s k procesu zvaném *crowdsourcing.* Což je *„centrálně organizovaná činnost, která vede k dosažení přesně definovaných cílů, a to s využitím většího množství zainteresovaných osob z řad zákazníků nebo sympatizantů, pocházejících z cílových skupin podle pole působnosti organizátora“.*[15] V případě metody human flash search je z výše uvedené definice cílem nalezení konkrétního jedince nebo skupiny obyvatel, případně vyvrátit nějaké tvrzení jedince nebo skupiny a sympatizanti jsou pak logicky nietzen, osoby vyhledávající. V této metodě tví obrovská síla právě v počtu zainteresovaných jedinců, kteří provádějí „detektivní“ činnost.
Cíle metody jsou podobné jako v případě doxingu, zveřejnění soukromých informací, odhalení totožnosti oběti, ponížení, zostuzení, často ale také její přímé potrestaní ať už formou kyberšikany nebo kyberstalkingu či dokonce potrestání přesahující do reálného světa, nezřídka kdy takové případy končí fyzickým napadáním či reálnými výhružkami újmou na zdraví.

Dalšími projevy, které by připadaly v úvahu a jistě jsou, byly a budou využívány digilantisty jsou například Phishing, Vishing, Smishing, Spear Phishing, Sniffing, DRDoS útoky (obdoba DoS a DDoS), Cybersquatting, Kyberstalking, Kyberšikana a mnoho dalších forem útoků, podvodů a projev, které lze v kyberprostoru použít k dosažení konkrétního cíle.

[15] Crowdsourcing. In: *SCS.ABC.CZ* [online]. Česká republika: 2005-2022 [cit. 5.12.2022]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/crowdsourcing

1.6 Vybrané skupiny, jednotlivci

1.6.1 ***Anonymous***

Počátky hnutí, které je dnes známé jako Anonymous, začaly vznikat v roce 2003 v Americe, a to díky webovým stránkám 4chan. Tento web – 4chan.org založil Christopher Pool, známý také pod přezdívkou moot. Jednalo se o webové fórum, jehož komunikace byla založena na obrázcích, pro tehdejší Ameriku vcelku neznámá a nepopulární záležitost, ovšem v Japonsku se podobný web s názvem 2chan (2chan.net, nebo také Futaba Chanel) těšil velké oblibě. Pro přesnost je nutné uvést, že Pool použil (zkopíroval) právě zdrojový kód 2chanu, který přeložil a nechal tak vzniknout neoficiální anglickou verzi tehdy populárního 2chanu.

4chan, web s nepřeberným množstvím vláken s různými tématy jako videohry, hudba, filmy, anime, politika, nevyžadoval po uživatelích žádnou registraci a všichni přispěvatelé v chatu byli označení jako „Anonymous“ a odtud pocházení název hnutí, které v překladu neznamená nic jiného než „anonymní“.

Část těchto anonymních uživatelů zprvu pouze tzv. trolila ostatní uživatele, tedy záměrně na diskuzních fórech vyvolávala hádky, provokovala svými výroky, zesměšňovala ostatní, prostě rušila jinak veskrze v té době běžný chat. Už tehdy ale malá skupina osob poznala, že mocnou zbraní na internetu je schopnost spolupráce velkého množství lidí. A zářný takový příklad, kdy hnutí organizovalo svou asi první „akci“ bylo zablokování online hry Habbo Hotel simulující fungování hotelu. Bylo to v roce 2006 a byl to jakýsi mix trolení a možná reakce na zákaz vstupu do bazénu malému chlapci s onemocněním virem HIV v USA. Nespočet uživatelů si zvolilo jako avatara postavu černocha a blokovali ostatním uživatelům přístup k bazénu a do hotelu s prohlášením, že je „uzavřen kvůli AIDS“. Později si hnutí začalo počínat více hacktivisticky a to díky tomu, že se Harold Turner, neo-nacista a komentátor rádiového pořadu Hal Turner Show nevybíravě vyjadřoval o uživatelích 4chanu. Anonymous prováděli DDoS útoky na jeho stránky, telefonovali mu do jeho pořadu, zjistili jeho soukromou adresu, na kterou mu začali posílat pizzu a stavební materiál, a to vše s cílem způsobit mu finanční škodu a

takto ho „zaměstnat“, aby nemohl financovat svou stanici a pokračovat ve vysílání.[16]

Následně už hnutí působilo přímo hacktivisticky, pouštěli se do různých operací a projektů, jak je sami nazývali. Nejznámější činnosti hnutí jsou:

- Project Chanology (2008) – vymezovali se proti praktikám Scientologické církve
- Operace odplata (2010) – podpora a hájení WikiLeaks
- Operace Sony (2011) – brání George Hotze, se kterým vedla Sony soudní spor kvůli prolomení zabezpečení herní konzole Playstation 3
- Účastnili se převratů v Tunisku a v Egyptě (2011)

V polovině roku 2011 byli někteří členové hnutí zatčeni. V této době se členové hlásili spíše ke skupině zvané LulzSec (viz. 1.6.), která se od Anonymous odštěpila.

Hnutí o sobě dalo vědět výrazněji v roce 2015, kdy oznámilo záměr postavit se Islámskému státu a pod heslem Operace Ice ISIS (#OpIsis, #OpParis) zveřejňovali a odstraňovali účty na sociální síti Twitter o nichž tvrdili, že patří přímo členům IS nebo jejich sympatizantům.[17] Z poslední doby je pak známá účast v kyberbojích proti Rusku pod názvem Operace Rusko (#opRussia), jako odveta za napadení Ukrajiny.

Symbolem hnutí se stala maska Guye Fawkese (jedna z hlavních osob zodpovědná za atentát na Skotského krále Jakuba I. dne 5.listopadu 1605), která byla použita ve filmu V jako Vendeta (2005), jež má komiksovou předlohu. Maska se tak stala typickou ikonou pro hnutí Anonymous stejně jako jejich slogan:

We are Anonymous	Jsme Anonymous
We are Legion	Jsme legie
We do not forgive	Neodpouštíme
We do not forget	Nezapomínáme
Expect Us	Očekávejte nás

[16] We Are Legion: The Story of the Hacktivists [dokument]. Režie Brian Knappenberger. USA/Velká Británie. 2012

[17] KARATZOGIANNI, Athina. Anonymous hackers could be Islamic State's online nemesis, In: *The Conversation.com*. 2015 [online]. [cit 6.12.2022]. Dostupné z: https://theconversation.com/anonymous-hackers-could-be-islamic-states-online-nemesis-50876

Hnutí Anonymous se svým počínáním v kyberprostoru stalo bezesporu prvním celosvětově známou vigilantní „skupinou“ a ačkoli došlo v roce 2011 k zatčení několika představitelů s hnutím jako takovým, s myšlenkou a jejich názory se defacto vůbec nic nestalo. Je to uskupení nezjištěného a proměnlivého počtu lidí. V určité podobě hnutí funguje i dnes, jelikož nemá a nikdy nemělo žádné hierarchické uspořádání, členové jsou na sobě nezávislí, neznají se osobně, pojí je jejich společný zájem a cíl, pro který v určitých situacích spolupracují a reaguje na dění ve světě.

1.6.2 Anonymous v České republice

V roce 2012 Anonymous působili i v České republice, zejména pak podnikali kyberútoky proti politickým stranám:

- provedli DDoS útok na webové stránky Ochranného svazu autorského (OSA – www.osa.cz). Byl to protest proti vybírání poplatků z každého kusu prodaného média, jako je CD, DVD atp.
- získali část osobních dat členů ODS, kterou zveřejnili (do medií uváděli, že získali všechna data všech členů).
- Získali přístup k webové stránce KSČM a její obsah nahradili vlastním textem, ve kterém voliče KSČM urážejí.
- Získali a zveřejnili osobní data tisíců členů ODS, včetně
- Prováděli DDoS útoky a webové stránky politických stran TOP09, ODS, ČSSD, KSČM, která na několik hodin vyřadili z provozu – jednalo se o tzv. Operaci zánik.[18]

Při vyhledávání Anonymous v síti Internet lze nalézt české příznivce Anonymous, kteří spíše sdílí informace a podporují hnutí. Příkladem na Facebooku může být stránka s názvem Anonymous Czech Republic (s posledním příspěvkem z března 2022), či Anonymous media cz (v současné době dohledatelná stránka bez aktivity) Anonymous CZ/SK (taktéž neaktivní) a mnohé další. Podobné je tomu i

[18] BESSER, Vilém. Kdo jsou vlastně vlivní hackeři Anonymous, kteří děsí svět. In: *Forum24* [online]. 2015 [cit. 6.12.2022]. Dostupné z: https://www.forum24.cz/kdo-jsou-vlastne-vlivni-hackeri-anonymous-kteri-desi-svet/

na sociální síti Twitter, Youtube, zájem je spíše mizivý, odběratelů a sledujících těchto kanálů je také velmi málo, oproti zahraničním skupinám, kde je sledujících v řádech desítek tisíc (př. @Anonymous9775 - Anonymous Kollektiv Germany) až milionů (př. @YourAnonNews) a aktivita kanálu výrazně vyšší.

Hnutí Anonymous je záměrně věnován největší prostor v této práci, domnívám se, že právě toto hnutí velmi výrazným způsobem zviditelnilo samotný pojem vigilantismu v kyberprostoru. Nezaměřuje se pouze na konkrétní oblast (jako například StopXam – viz 1.6.1). Je to hnutí, využívající širokou škálu metod k dosažení svých cílů. Ačkoli si hnutí počíná protiprávně, třebaže s ušlechtilým záměrem, v očích veřejnosti je ochráncem hodnot, spravedlnosti, spravedlivé odplaty.

1.6.3 ***LulzSec***

LulzSec byla poměrně malou skupinou hackerů odtrženou od hnutí Anonymous, její jádro tvořila šestice osob a variabilní počet přibližně deseti až dvaceti dalších hacktivistů, kteří spolupracovali. Mezi zakládající členy patřily osoby tehdy známé pod přezdívkami Topiary, Sabu, Tflow, Kayla. [19]

Samotný název skupiny je složen ze dvou slov, tím prvním je jakýsi novotvar výrazu „lol“ (laugh out loud neboli hlasitě se smát) a druhým slovem je „Security“ česky bezpečnost. Skupina někdy nazývána také jako LulzSecurity. Jejich symbolem byl jednoduchý černobílý obrázek zobrazující horní část těla gentlemana s knírem, v obleku s kravatou a brýlemi na jedno oko na šňůrce, tzv. monokl, pozvedávající sklenici vína. Tento meme je používaný dodnes.

Jak se jistě dá se samotného názvu skupiny soudit, její útoky byly kombinací aktivismu na internetu a humoru. Humorná část měla pobavit samotné aktéry a širokou veřejnost, což se jim za jejich krátkého působení v roce 2011 dařilo. Byli velice aktivní na sociálních sítích, zejména na Twitteru, kam jejich mluvčí Topiary přidával příspěvky každý den. Jejich útoky oběti zesměšňovali a uráželi, mnohdy připojili na nabourané stránky i osobitý text stejně jako při jejich prvním útoku z května 2011. Tehdy překonali zabezpečení stránek televizní společnosti Fox

[19] OLSON, Parmy. J*sme Anonymous,* Praha: Práh, 2012, ISBN 978-80-7252-400-6

News, přisvojili si osobní informace o soutěžících z pořadu X Factor a na stránkách zanechali vzkaz: „We don't like you very much. As such, we cordially invite you to kiss our hand-crafted crescent fresh asses" („Moc rádi vás nemáme, srdečně vás proto zveme k políbení našich půlek"). Byla to jejich reakce na tehdejší kritiku televizní společnosti vůči rapperovi Commonovi (Lonnie Rashied Lynn). Mezi jejich další známé útoky můžeme zařadit krádež údajů 3100 bankovních účtů ve Velké Británii, útoky vůči společnosti Sony, zveřejnění hesel skoro tří desítek tisíc uživatelů pornografických webů, útočili na společnost PBS po odvysílání negativního pořadu na WikiLeaks, napadli i Infragard, pobočku FBI, zde poškodili webové stránky a přisvojili si e-maily a osobní údaje jednoho ze zaměstnanců. Krátce na to, v polovině roku 2011, FBI vypátrala jednoho z hlavních členů skupiny, Sabua – osobu Hector Monsegur (zapomněl při jednom z útoků použít nástroj k maskování svého umístění v síti). Monsegur následně spolupracoval s FBI, což víceméně vedlo k zániku celé skupiny.[20]

Další členové, představující jádro hnutí bylo zatčeni policií, jednalo se o osoby Jake Davis alias „topiary", „atopiary", Ryan Ackroyd alias „kayla", „lol", „lolspoon", Darren Martyn alias „pwnsauce", „reapsauce", „networkkitten", Donncha O'Cearrbhail, alias „palladium".[21]

1.6.4 ***StopXam***

Jedná se o ruské aktivistické hnutí, které v roce 2010 založil Dmitrij Alexandrovič Čugunov, známé také pod názvy StopHam nebo Stop a Douchebag v překladu znamenající „Zastav hulváta". Mladí aktivisté vybavení kamerami a samolepkami bojují proti agresivním řidičům v Rusku, zejména těch, kteří jezdí nebo parkují na chodnících. Řidiče páchající takové přestupky zastavují, snaží se je upozornit na jejich protiprávní jednání a přimět ke slušnosti, dostávají se tak do častých konfliktních situací. Jednání řidičů i případný konflikt si skupina aktivistů natáčí na kameru. Na čelní sklo neposlušných řidičů často lepí těžko odstranitelné velké

[20] GREGORY, Jennifer. 10 Years Later, What Did LulzSec Mean for Cybersecurity?. In: *Security Intelligence* [online]. © 2022 IBM [cit. 6.12.2022]. Dostupné z: https://securityintelligence.com/articles/lulzsec-10-years-later-cybersecurity-influence-meaning/

[21] Leading Member of the International Cyber Criminal Group LulzSec Sentenced in Manhattan Federal Court. In: *FBI Federal Bureau of Investigation* [online]. 2014 [cit. 6.12.2022]. Dostupné z: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/leading-member-of-the-international-cyber-criminal-group-lulzsec-sentenced-in-manhattan-federal-court

kulaté samolepky s nápisem v českém jazyce znamenajícím: „Na všechny kašlu. Řídím a parkuji, kde a jak chci!“ Většina řidičů se po jejich kontaktování omluví, ale jsou i tací, kteří naopak reagují přehnaně, vulgárně, vyhrožují aktivistům újmou na zdraví či dokonce smrtí. Sestříhaná videa pak zveřejňují na YouTube, čímž se snaží neslušné, protiprávně jednající řidiče, potrestat formou zveřejnění a zároveň poukázat na problém a změnit chování ostatních řidičů v Rusku.[22]

Na Youtube přidávají krátká videa (okolo 10 minut, ale i delší). Jejich hlavní kanál s názvem СтопХам (@stopxamlive) má v současné době 1,74 milionů odběratelů a jejich nejpopulárnější videa mají desítky milionů zhlédnutí, Kanál s názvem StopXam Msc (@StopaDouchebag) s 881 tisíci odběrateli má rovněž vysokou návštěvnost. Lidé jejich tvorbu podporují prostřednictvím Patreonu (platforma díky níž může fanoušek finančně podpořit tvůrce videí) nebo i nákupem jejich merche (zkrácenina slova „merchandise“ – zboží).

Dá se říci, že aktivisté StopXam jsou na pomezí klasického vigilantismu a kybervigilantismu. Fakticky konfrontují neslušné či přestupek páchající řidiče, lepí jim samolepky na čelní skla, vystavují řidiče určitému nepohodlí, před ostatními účastníky silničního provozu s nimi řeší jejich chování na silnici, natáčí si je, sami se stávají terčem vulgarit a výhružek. A vše to, co zaznamenali na kamery v reálném světě, pak přenesou do toho virtuálního. Ukáží ostatním chování agresivních řidičů, jejich podobu, podobu případného spolujezdce typ vozidla i registrační značku.

*1.6.5 **Česká alternativa***

Jelikož jsou videa tohoto druhu na YouTube velice populární nejen v Rusku, ale všude ve světe, existuje i několik velmi populárních kanálů s podobnou tématikou také v České republice. Za zmínku stojí například kanál s názvem Liberecká perla (@LibereckaPerla). Autor videí pomocí kamery ve vozidle zaznamenává přestupky ostatních účastníků silničního provozu, které pak v první části videa zveřejní někdy i s titulky pro lepší pochopení kontextu případně video doplní o

[22] VODRÁŽKA, Prokop. Rusové bojují proti agresivním řidičům. Podpořil je i Putin. *In: Aktuálně.cz* [online]. Praha, 2015 *[cit. 7.12.2022]. Dostupné z: https://magazin.aktualne.cz/rusove-bojuji-proti-agresivnim-ridicum-podporil-je-i-putin/r~bcc4cb761f3611e58a300025900fea04/*

vlastní komentář. V druhé části videa pak zveřejňuje videa jemu zaslaná, pořízená ostatními řidiči sledující jeho kanál. Kanál má v současné době 73,7 tisíc odběratelů a nejpopulárnější videa mají několik set tisíc zhlédnutí. Autor, očividně znalý pravidel silničního provozu, se v některých videích zabývá i zažitými chybami českých řidičů a různými spornými otázkami ze silnic. Druhým příkladem může být velice podobný kanál s názvem Plzeňská Jehlárenská (@PlzenskaJehlarenska) s velmi podobným obsahem se 114 tisíci sledujícími.

Hlavním rozdílem mezi českými zástupci poukazujícími na chyby a přestupky ostatních řidičů oproti ruským aktivistům je fakt, že čeští tvůrci videí nevstupují dobrovolně osobně do konfliktních situací, ale natáčejí problematické jednání na kameru ve vozidle a videa následně zveřejňují na YouTube.

*1.6.6 **Kitboga***

Kitboga je přezdívka amerického streamera, youtubera, tvůrce vidí působícího zejména na platformě Twich (živé vysílání) a YouTube. Aktivní je ale i na ostatních sociálních sítích jako je Twitter, TikTok, Instagram, Facebook, Reddit. Na Youtubovém kanále Kitboga (@KitbogaShow) má 2,94 milionů odběratelů a jeho videa dosahují stovek tisíc zhlédnutí. Na Twichi má přibližně 1,2 milionů sledujících.

Jeho tvorba se zaměřuje především na podvádění podvodníků na internetu humornou formou. Na sociálních sítích takto působí od roku 2017, jeho skutečné jméno není známo, soukromí si pečlivě střeží, ačkoli jeho tvář zná miliony lidí.

Ve svých několikahodinových streamech si dělá prostřednictvím tel. hovorů legraci z internetových podvodníků a zdržuje je od jejich „práce“, používá softwarový nástroj na úpravu hlasu a předstírá tak mnoho různých osob (např. starou dámu). Podvodníci se skutečně domnívají, že hovoří s reálným člověkem, kterého se snaží okrást o úspory. Na YouTube nahrává sestříhanou nejzábavnější část, kde uživatelům i vysvětluje podvodné praktiky.

Kitboga je přímo ukázkový scambaiter, který své počínání navíc zaznamenává a sdílí ho pro zábavu a osvětu s ostatními uživateli sociálních sítí.

*1.6.7 **WikiLeaks***

Sama sebe na svém webu WikiLeaks prezentuje jako mezinárodní mediální společnost přinášející důležité informace a zprávy v necenzurované podobě veřejnosti, specializují se na válku, špionáž a korupci. Zveřejnili více než 10 milionů dokumentů. Jejím zakladatelem se stal v roce 2006 Julian Assange.[23]

Server v roce 2010 zveřejnil 80 tisíc dokumentů týkajících se války v Afghánistánu a následně o několik měsíců později tajné vojenské dokumenty z války v Iráku z období let 2004 – 2009, což bylo pro tehdejší veřejnost šokující odhalení. Z dokumentů vyplývaly informace o týrání, vraždách, znásilnění vězňů iráckými policisty a vojáky i americkými úřady, rovněž došlo k odhalení zabíjení civilistů americkou soukromou bezpečnostní službou Blackwater.[24]

Mezi největší odhalení WikiLeaks patří zejména:

- V roce 2007 byla odhalena 238stránková příručka z roku 2003 s názvem „Aproval of Camp Delta Standard Operating Procedure (SOP)“ - „Schválení standardního postupu pro tábor Delta“ – ze které vyplývalo ukrývání některých vězňů před inspektory Červeného kříže, aby byli následně pro vyšetřovatele poddajnější.
- V roce 2009 server zveřejnil obsah 570 tisíc pagerových zpráv z 11. září 2001, které si vyměnili zaměstnanci Pentagonu, FBI, FEMA a NYPD.
- V roce 2010 server zveřejnil video z hlavního města Iráku zachycující střelbu amerického vrtulníku Apache do civilistů, při které byl mimo jiných osob zabit i fotograf agentury Reuters.
- Na přelomu let 2010 a 2011 došlo ke zveřejnění 250 tisíc depeší z let 1966 – 2010, ze kterých vyplývaly tajné útoky drony v Jemenu, snaha získat podrobnosti o představitelích OSN a dále např. popis Ruska jako „virtuálního mafiánského státu“.

[23] What is WikiLeaks. In: *WikiLeaks* [online]. 2015 [cit. 7.12.2022]. Dostupné z: https://wikileaks.org/What-is-WikiLeaks.html

[24] SOBOLA, Ondřej. Před 10 lety server WikiLeaks zveřejnil utajované vojenské dokumenty o válce v Iráku, Assange teď čeká na soud o vydání do USA. In: *Česká televize* [online]. 2020 [cit. 7.12.2022]. Dostupné z: https://ct24.ceskatelevize.cz/svet/3212524-pred-10-lety-server-wikileaks-zverejnil-utajovane-vojenske-dokumenty-o-valce-v-iraku

- V roce 2016 došlo ke zveřejnění celkem 22 tisíc e-mailů s kompromitujícími informacemi Demokratického národního výboru USA.[25]

V prosinci 2010 společnosti jako Visa, MasterCard a PayPal přestaly spolupracovat s WikiLeaks, od podporovatelů tak nemohla prostřednictvím těchto společností přijímat finanční prostředky, což jí způsobilo nemalé finanční potíže. Na tuto skutečnost reagovalo i hnutí Anonymous a formou „Operace odplata" prováděli DDoS útoky na webové stránky těchto společností, která se stávaly nedostupnými.

Hlavní tvář WikiLeaks a její spoluzakladatel Julian Assange čelí od prvních zveřejněných dokumentů trestním stíháním, 7 let strávil na ekvádorském velvyslanectví a od roku 2019 se nachází ve výkonu trestu odnětí svobody ve Velké Británii. Spojené státy Americké neustále usilují o jeho vydání

[25] CUMMINGS, William. Six big leaks from Julian Assange's WikiLeaks over the years. In: *USA Today News* [online]. 2019, USA [cit. 7.12.2022]. Dostupné z: https://eu.usatoday.com/story/news/politics/2019/04/11/julian-assange-six-wikileaks-most-memorable-revelations/3434371002/

2 PRAKTICKÁ ČÁST

2.1 Internetoví detektivové

2.1.1 ***Wang Jue***

První případ metody Human flash search, který si získal obrovskou pozornost, byla událost z počátku roku 2006. Tehdy se mezi obyvateli Číny začalo šířit video zachycující ženu ve středním věku, Asiatku spoře oděnou na jehlových podpatcích držící v rukou malé kotě. Na videu se usmívala, po krátké chvíli kotě položila na zem a podpatkem mu dupala na hlavu, dokud kotě nezemřelo.[26] Nutné je zmínit, že videa podobného typu nebyla v Číně (i jinde ve světě) v onu dobu, a i v tu dnešní ničím výjimečným, jedná se o formu kybersadismu a tvůrci těchto videí na nich vydělají nemalé finanční prostředky. Video se okamžitě stalo předmětem diskuze na chatovacích a diskuzních čínských platformách, kde ho lidé odsuzovali, volali po trestu účinkující ženy a začali se ptát, zdali jí někdo nezná. Tím začali „vyšetřování“ v kyberprostoru. Z přání smrti aktérce se příspěvky stávaly praktičtější a lidé se snažili identifikovat místo, kde k činu došlo. Po čtyřech dnech pátrání jí poznal člověk pocházející ze stejného města a přidal tento příspěvek do diskuzního fóra. A během dalších dvou dnů se uživatelům podařilo ztotožnit zdravotní sestru Wang Jue z provincie Heilongjiang Došlo ke zveřejnění jejího jména, telefonního čísla, jejího bydliště i zaměstnavatele. Nemocnice s ní rozvázala pracovní poměr a na webových stránkách města, kde žena žila byla zveřejněna omluva za její chování. Samotná Wang pak čelila nespočtu urážek a výhružek smrtí, ze svého bydliště se odstěhovala.

2.1.2 ***Yin Feng***

Druhý případ, rovněž z Číny, je z roku 2013 a týká se taxikáře, který ze svého vozu přes stažené okénko řidiče plivl na povalujícího se bezdomovce. Svědci této události si zapamatovali část registrační značky vozidla taxi a podělili se se svým zážitkem na sociálních sítích, a tak začal hon na nevhodně se chovajícího řidiče.

[26] DOWNEY Tom. China’s Cyberposse, In: *The New York Times Magazine* [online]. New York, 2010 [cit. 8.12.2022]. Dostupné z: https://www.nytimes.com/2010/03/07/magazine/07Human-t.html

O pouhých několik hodin později byl digilantisty vypátrán Yin Feng, řidič vozila taxi služby, jehož část registrační značky se opravdu shodovala s tou původní zaznamenanou. Veškeré dostupné osobní údaje řidiče byly zveřejněny, zejména jeho telefonní číslo, na které mu neustále telefonovali rozhořčení lidé, kteří mu nejen kázali o morálce ale i ho finančně vydírali.[27] Jedná se o další metodu Human flash search kombinovanou s doxingem, která byla použita, ovšem v tomto konkrétním případě byl vyhledán nevinný člověk, který se jednání nedopustil. Řidič Feng byl vystaven kyberšikaně, kyberstalkingu aniž se dopustil shora popsaného jednání. Byl jen výsledkem chybného doxingu digilantistů.

*2.1.3 **Luca Magnotta***

Třetím případem je případ skutečného vraha jménem Luca Magnotta, který má jak jinak svůj počátek v síti Internet. „1 boy 2 kitten“ byl název videa zveřejněného v roce 2010 na YouTube, ve kterém osoba v zelené mikině s kapucí umístí 2 koťata do vakuového těsnícího pytle, ze kterého následně odsaje vzduch, čímž se koťata udusí. Uživatelé sociální sítě Facebook o videu zprvu diskutovali, odsuzovali a následně založili facebookovou skupinu věnující se vypátrání pachatel týrání zvířat. Nejvíce diskutujícími členy byla Deanna Thompson, alias „Baudi Moovan“ a Johgn Green, takřka obyčejní lidé trávící nespočet hodin svého volného času na sociálních sítích. Všímali si detailů z videa, rozmístění nábytku, použitého vysavače atp. Postupem času se jim podařil vypátrat profil na Facebooku jménem Jamesey Cramsalot Inhisass, fotografie uživatele profilu nápadně připomínala osobu z videa. Díky velkému množství uživatelů ve skupině, přibližně okolo 15000 lidí, kteří se do vyhledávání zapojili se skupině brzy podařilo zjistit skutečné jméno osoby – Luca Rocco Magnotta. Magnotta poté zveřejnil další video s kočkou, kterou utopil. Na začátku května 2012 jeden ze členů skupiny sdílel video (tehdy se šířilo pod názvem „1 Lunetic, 1Ice Pick“) na němž je zaznamenána skutečná vražda. Obětí byl 33letý student univerzity Concoridia v Montréalu, později policií ztotožněný jako Jun Lin. Lin byl na videu jinou osobou

[27] HATTON, Celia. China's internet vigilantes and the 'human flesh search engine'. In: *BBC* [online], Peking, 2014 [cit. 9.12.202]. *Dostupné z: https://www.bbc.com/news/magazine-25913472*

ubodán kuchyňským nožem a sekáčkem na led. Jeho tělo bylo následně rozřezáno a některé části jeho těla byly rozeslány Kanadským úřadům. Facebookovou skupinou byla shledána podobnost s videi s utýranými zvířaty a vraždu od počátku přisuzovala Magnottovi. Pokračovala v hledání digitálních stop a elektronicky kontaktovala policii. Místní policie se případem začala intenzivně zabývat až ve chvíli, kdy bylo nalezeno tělo oběti. Později policie požádala o přidání do facebookové skupiny, kde nalezli spoustu digitálních stop. Díky rozsáhlému pátrání policie a pomoci digilantistů byl Magnotta dopaden v červnu 2012 v Berlíně. Na základě události byl natočen i třídílný snímek z produkce streamovací společnosti Netflix s názvem „Don't F**k with Cats: Hunting an Internet Killer“ (Od koťátek pracky pryč! Hon na internetového zabijáka!).

Je zřejmé, že všechny tři vyhledané případy jsou formou vigilantismu v kyberprostoru. Byly při nich použity metody doxing a human flash search. V síti Internet lze nalézt nespočet podobných případů. Jedná se o extrémně funkční metodu, která je efektivnější tím, čím více lidí se do ní zapojí. Mohli bychom polemizovat o tom, že čím více zapojených uživatelů, tím více je získáno relevantních dat, ale také dat nesprávných, pořád to ale budou data úměrná k počtu připojených uživatelů, nevyhodnocuje je jen jeden člověk, ale vždy celá skupina. Na druhém příkladu je zřejmé, že i když se jedná o efektivní metodu, ne vždy je nalezen skutečný „viník“ a vigilantisté se tak ženou potrestat první nalezenou oběť, v tom tkví jedno z hlavních nebezpečí, touha někoho potrestat může převažovat nad pečlivým vyhledáním skutečného „viníka“. Tím druhým nebezpečím je pak samotné potrestání „viníka“ neboli oběti vigilantismu, které je ve většině případů pro dotyčného zdrcující v osobním, pracovním, ale i v sociálním směru.

Rizika: Jednoznačně největším rizikem je možnost označení nesprávné osoby. Dalším rizikem pak může být vznikání nebezpečných sociálně patologických jevů jako je šikana (kyberšikana) a s tím související možnost protiprávního jednání vůči nalezené oběti, vyhrožování újmou na zdraví a životě, vydírání, možné fyzické napadání v reálném světě atp.

Následky: Následky pro oběť bývají velkým zásahem do jejího soukromí, ovlivnit to může jak osobní, tak i pracovní stránku. V řadě případů je věc medializována nebo jiným způsobem výrazně zviditelněna, a tak je oběť často prověřována i policií. V případě, že se jedná o skutečného pachatele protiprávního jednání, bývá trestán dvakrát. Poprvé tím zviditelněním jeho osoby v kyberprostoru a následně také rozhodnutím soudů či jiných orgánů.

2.2 Hon na pedofily

*2.2.1 **Letzgo Hunting***

V současné době zaniklá skupina, která na svých stránkách letzgohunting.com, které jsou dlouhou dobu nedostupné sama sebe charakterizovala následovně:

„Letzgo Hunting je oddaná skupina lidí, kteří se snaží odhalit prohnané a bezohledné jedince, jako jsou pedofilové, nebo kohokoli, kdo může být hrozbou pro naše děti.

Pracujeme v rámci zákonných omezení, abychom tyto odporné lidi odhalili, zveřejnili a postavili před soud pomocí síly internetu a videokamer.

Kdykoli to bude možné a při každé příležitosti budeme vás, širokou veřejnost a naše příznivce, informovat o našich aktivitách a "úlovcích", a to zveřejňováním videozáznamů, fotografií a údajů ze zpráv na sociálních sítích na našich webových stránkách (Letzgohunting.com) nebo na jiných sociálních sítích, jak uznáme za vhodné. (tj. Facebook, Youtube, Liveleak atd.).

Členové našeho „zásahového týmu" mají anonymní individuální profily a v současné době je tvoří:

Scumm Buster, Facee Buster a Keeboo Buster.“

Tyto členy můžeme čas od času doplnit nebo změnit, jak uznáme za vhodné.“[28]

Jednalo se o skupinu osob z Anglického metropolitního hrabství Leicestershire, které se na internetu vydávala za mladistvé dívky. Předstírající mladistvé pak navazovala konverzace s muži, kteří vyhledávali sexuální konverzaci a snažili se s dítětem navázat i osobní kontakt. Jedním z mužů, se kterým si skupina takto dopisovala byl i Gery Cleary na začátku roku 2013. Na osobní schůzce, kam byl

[28] About Us. In: *Wayback Machine* [online]. 2013 [cit.10.12.2022]. Dostupné z: https://web.archive.org/web/20130417180227/http://letzgohunting.com/view_page.php?pid=1

vylákán ho skupina konfrontovala, přičemž jednání zaznamenávala na kameru. Záznamy poté byly zveřejněny na sociálních sítích a předány policii. V průběhu května 2013 byl Gery Cleary zatčen místní policií a následně propuštěn na kauci. Policií nebyl obviněn z žádného trestného činu. Čtyři dny po svém zatčení spáchal Gary Cleary sebevraždu oběšením.[29]

2.2.2 ***V síti***

Velmi zajímavou formu, která by se pravděpodobně dala označit jako digilantismus (možná na pomezí sociálního experimentu s prvky digilantismu), představil v roce 2020 Vít Klusák spolu s Barborou Chaloupkovou v dokumentárním snímku *V síti* věnující se zneužívání dětí na internetu. V díle se věnují zejména dvěma fenoménům, a to kybergrooming a sexting. Kybergrooming je „*manipulace dítěte v online prostředí jinou osobou s cílem přesvědčit ho k osobní schůzce v reálném světě*“[30]. Sexting „*označuje dobrovolné sdílení intimních materiálů jako fotografií, videí, případně sexuálně explicitního textu s jinými osobami*“[31].

Digilantisty se v podstatě stali všichni členové podílející se na natočení snímku.

V dokumentu účinkuje trojice dospělých hereček, které ovšem vypadají výrazně mladší, než jakými doopravdy jsou, čemuž ve snímku dopomůže i oblečení a vytvoření kulis, tedy dětských pokojíčků. Ve filmu tyto ženy ztvárňují dvanáctileté dívky, jsou jim vytvořeny profily na sociálních sítích a je dokumentována jejich komunikace zejména s muži, kteří je oslovují. Bohužel nebylo překvapením, že většina mužů, kteří dívky oslovili, s nimi hovoří v sexuální rovině, požadují po nich jejich nahé fotografie, sami posílají své, masturbují před nimi a snaží se je vylákat k osobní schůze, vydírají je atp. V dokumentu nebyla odhalena totožnost těchto mužů, sexuálních predátorů, jak byli nazýváni. Jejich obličeje byly rozmazány, hlasy pozměněny, označováni nebyli skutečnými jmény, ale přezdívkami, z těch nejpopulárnějších to byl tzv. „Ústečan“, „Sneeky“. V některých případech se dívky

[29] Letzgo Hunting denies blame for man's suicide. In: *BBC* [online]. 2013 [cit. 11.12.2022]. Dostupné z: https://www.bbc.com/news/uk-england-leicestershire-24145142

[30, 31] O čem je film V SÍTI. In: *Dokument V síti* [online]. [cit. 11.12.2022]. Dostupné z: https://vsitifilm.cz/jsem-rodic.html

s filmovým štábem (maskovaným) osobně setkaly s predátory a došlo ke konfrontaci.
Celkem se dívkám během 10 dnů natáčení ozvalo 2458 mužů. Po odvysílání dokumentu jeho tvůrci spolupracovali s policií. [32]
Zajímavé bylo, že vzápětí premiéry filmu v kinech se na sociálních sítích sami predátoři stali předmětem doxingu a tak v jednu chvíli byla známa některá reálná jména predátorů, která i dnes lze vcelku jednoduše vyhledat.

Při hledání příkladů na internetu bylo nalezeno hned několik skupin, kteří se zabývají vyhledáváním pedofilů, předávání informací policii a většinou tuto činnost spojují i s nějakou podívanou, kterou umisťují na sociální sítě. Kromě Letzgo Hunting lze zmínit i skupinu Deamon Hunter nebo „lovce“ nazývaného Stinson Hunter, organizace Terres des Hommes a jejich virtuálně vytvořená desetileté holčička Sweetie. Zahraniční alternativou dokumentu k síti by pak mohl být seriál nebo reality show s názvem To Catch a Predator.

Rizika: Opět zde hrozí, že může být označena nesprávná osoba, že může vznikat řada sociálně patologických jevů vůči vypátraným jedincům. Rizikem může být i vznikání dalších vigilantních projevů, zejména v případech, ve kterých si digilantisté myslí, že trest pro pachatele je nízký, nedostatečný nebo, že trest dosud nebyl vykonán, a tak vzniká možnost „braní zákona do vlastních rukou“ a trestat podezřelou osobu nebo „nečinné“ orgány (policii, soud, státní zastupitelství).
Následky: Pro neprávem (i po právu) označeného člověka může mít takové označení drtivý dopad, mnohem závažnější než v předchozích případech, v některých případech si takto neprávem označení lidé sáhnou na život. Druhý příklad je ovšem ukázkou toho, že se může podařit vypátrat skutečné osoby páchající trestnou činnost na dětech a vhodnou spoluprací s orgány činnými v trestním řízení jsou takové osoby spravedlivě potrestány. Následky tedy mohou

[32] Policie kvůli dokumentu V síti vyšetřuje sexuální predátory. Jeden už od soudu odešel s trestem. In: *iROZHLAS – spolehlivé zprávy* [online]. 1997-2022 [cit. 23.1.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/v-siti-dokument-film-vit-klusak-barbora-chalupova-policie-podezreli_2002181141_dok

být pro společnost i příznivé, v jisté formě je provedena osvěta obyvatel (zvláště pak rodičů o tom, co jejich dítěti může hrozit na internetu) a zároveň dochází k potrestání skutečných pachatelů.

2.3 Operace Sony

Na začátku roku 2011 se stala společnost Sony obětí jednoho z největších útoků DDoS útoku ze strany hnutí Anonymous. Vše začalo sporem společnosti Sony s Georgem Francisem Hotzem alias „geohot“, který jako první člověk překonal zabezpečení tehdejší herní konzole Playstation 3, což mohlo vést ke spouštění jiných operačních systémů v zařízení, instalaci aplikací, spouštění pirátských her atd. Geohot následně zveřejnil video, kde své tvrzení dokazuje a na svých webových stránkách i manuál k odemčení zařízení Playstation 3 následkem čehož ho Sony v lednu roku 2011 zažalovala. Podle hnutí Anonymous Geohot odhalením slabiny v zabezpečení prokázal společnosti Sony obrovskou službu. Vedly se diskuze na téma, zda uživatel, který si zakoupil hardware, si s ním může nakládat, jak uzná za vhodné, a tedy i zasahovat do firmwaru, softwaru. Hnutí Anonymous také vadilo, že v průběhu řízení spol. Sony získala Geohotova data z Youtube, Twitteru a jeho vlastních webových stránek. Jak bývalo pro Anonymous typické, hnutí vydalo krátké prohlášení, ve kterém hrozí spol. Sony odplatou. V dubnu téhož roku začalo hnutí útočit na servery spol. Sony DDoS útoky, což ve výsledku vyústilo k výpadku služby Playstation Network (služba, díky které uživatelé tehdejší uživatelé Playstation 3 mohli nakupovat a stahovat digitální média, především hry. Ve službě měli uložené informace o svém profilu, mimo jiné také informace o platebních kartách). Služba Playstation Network nebyla pro hráče dostupná několik dlouhých týdnů. Později vyšlo najevo, že během útoků byla získána data 77 milionů uživatelů včetně údajů z platebních karet. Společnost Sony tehdy čelila drsné kritice ze strany uživatelů, kteří byli rozhořčení jednak nedostatečným zabezpečením jejich služeb a také nemožností několik týdnů plnohodnotně používat Playstation 3. V průběhu následujících měsíců vycházely najevo i skutečnosti o nedostatečném zabezpečení serverů Sony proti únikům dat. Jelikož všichni uživatelé museli po útocích obnovit svá hesla, docházelo

k opětovným pádům serverů služby Playstation Network v řádech několika dní.[33] Podle agentury Reuters byla společnosti Sony způsobena škoda ve výši 175 milionů dolarů. Mezi značnou část nákladů spadá především najímání externích analytických společností, opravy a výměny počítačů.[34]

Prakticky každý den dochází k útokům DDoS. Jakékoli služba poskytované prostřednictvím internetu (e-mail, webové stránky, cokoli se nachází v síti) může být útoky zpomalena nebo zcela vyřazena. Počet útoků DDoS se neustále zvyšuje, v roce 2018 bylo zaznamenáno 7,9 milionů útoků DDoS a v roce 2022 je jejich počet už 15,4 milionů.[35]
Jedná se tedy o často používanou metodu v síti Internet, a to nejen digilantisty. Výše uvedený příklad není nijak ojedinělou záležitostí. Postup DDoS je vždy velice podobný, proto nemá smysl uvádět další příklady. „*Pachatelé vyžívají k útoku koordinovanou síť distribuovaných kompromitovaných zařízení (tzv. botnet síť tvořenou zombie počítači). S využitím řídících serverů (C&C = Command and Control) posílají přes botnet na dálku nevyžádané požadavky v řádu až terabitů za sekundu. Snaží se zaměřit pozornost na síťové prvky systémů, které jsou nezbytné k navázání internetového připojení (např. router) případně na webové stránky, servery či databáze, dokud se jim nepodaří systém přetížit*.“[36]

*2.3.1 **Právní kvalifikace DDoS útoků***

Ačkoli to nebylo přímo cílem této práce, během zkoumání praktických příkladů byla zjištěna zvláštnost v právní kvalifikaci DDoS útoků v České republice. Postihovány jsou zejména podle trestního zákoníku, konkrétně pak podle § 230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do

[33] PHILLIPS, Tom. Five years ago today, Sony admitted the great PSN hack. In: *Eurogamer* [online]. 2016, [cit. 24.1.2023]. Dostupné z: https://www.eurogamer.net/sony-admitted-the-great-psn-hack-five-years-ago-today
[34] RICHWINE, Lisa. Cyber attack could cost Sony studio as much as $100 million. In: *Reuters* [online]. 2014 [cit. 24.1.2023]. Dostupné z: https://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209
[35] NICHOLSON, Paul. Five Most Famous DDoS Attacks and Then Some. In: *A10 Networks* [online]. 2022 [cit. 24.1.2023]. Dostupné z: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
[36] DDoS útok. In: *Eset* [online]. Praha, 1992-2023 [cit. 24.1.2023]. Dostupné z: https://www.eset.com/cz/ddos-utok/

počítačového systému nebo nosiče informací, kde je v prvních dvou odstavcích uvedeno:

„(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.*

(2) *Kdo zasáhne do počítačového systému nebo nosiče informací tím, že*

a) *neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*

b) *data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými*“.[37] Tato formulace je účinná od 28.6.2022, do té doby ovšem zákonodárce vyžadoval, aby pachatel DDoS útoků „neoprávněně získal přístup k počítačovému systému“, což se v případě DDoS útoků nikdy neděje, útočníci nezískávají přístup k počítačovým systémům, pouze velmi jednoduše řečeno zahlcují počítačový systém opakovanými požadavky tak, aby nebyl schopný reagovat na požadavky legitimních uživatelů internetu. Do 28.6.2022 tak nebylo možné postihnout útočníky DDoS útoků podle § 230 trestního zákoníku. Zákonodárce tak vcelku dlouhou dobu nereagoval dostatečně na Sdělení ministerstva zahraničních věcí č. 104/2013 Sb. o sjednání Úmluvy o počítačové kriminalitě, konkrétně na článek 5, 1. oddílu, druhé kapitoly: „*Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat*.“[38]

Rizika: V případě, že se do DDoS útoků zapojí mnoho uživatelů, např. na základě výzvy na sociálních sítí, nebo jsou útok prováděny obrovským množstvím botnetů, je útok takřka neodvratitelný. Rizikem může být i to, že provádění DDoS útoků má

[37] Zákon č. 40/2009 Sb., Trestní zákoník. In: *Zákony pro lidi* [online]. © AION CS, 2010-2023 [cit. 25.1.2023]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2009-40

[38] Sdělení č. 104/2013 Sb. m.s., *Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě*. In: *Zákony pro lidi* [online]. © AION CS, 2010-2023 [cit. 25.1.2023]. Dostupný také z: https://www.zakonyprolidi.cz/ms/2013-104

za cíl pouze odvést pozornost od jiného jednání, např. krádeže osobních údajů ze serverů. Donedávna hrozilo i riziko nemožnosti takové útoky postihovat v souladu s trestním zákoníkem. Dalšího vcelku výrazné riziko bylo zjištěno právě v souvislosti s útoky na ruské propagandistické servery, či jiné instituce. Po začátku války se na sociálních sítích i na diskuzních fórech šířili odkazy a výzvy k připojení se k útokům na „Rusko“. Výzvy obsahovaly návod, jak takový útok uskutečnit, a i pro méně zkušeného uživatele by nebyl problém zapojit se do takového jednání. Problém ovšem spočíval v tom, že DDoS útoky nesměřovaly pouze na cíle (servery) v Rusku, ale předmětem útoku byly i jiné servery v jiných zemích, také například webové stránky českých institucí a orgánů.

Následky: Škoda pro oběť DDoS útoků z pohledu trestního zákoníku může dosahovat od částek menších, než je škoda nikoli nepatrná, ale také se může vyšplhat až k částce přesahující škodu velkého rozsahu (jako v popsaném případě z roku 2011, kdy se obětí stala spol. Sony). Můžeme uvažovat, zda mohou být DDoS útoky ze strany digilantistů prospěšné např. v případě napadání ruských serverů v období právě probíhající války mezi Ruskem a Ukrajinou. Z pohledu Ruska taková činnost jistě žádoucí není, druhá strana tento typ útoku jistě vítá, ne-li přímo podporuje.

2.4 Zábavná videa ze silnic

Každý týden YouTubový kanál s názvem Liberecká Perla a Plzeňská Jehlárenská zveřejní minimálně jedno přibližně desetiminutové video z českých silnic zobrazující přestupky účastníku silničního provozu. Není to výsada pouze těchto dvou kanálů na platformě YouTube, ale mnoho českých, a především zahraničních kanálů takováto videa zveřejňuje. Je to určitý druh zábavy, lidé podobná videa vyhledávají, baví se jimi, komentují je. V některých videích jejich tvůrci zakrývají obličeje účastníků případně registrační značky vozidel v jiných záměrně nikoli. Záměr umisťování videí s touto tématikou může být různý a má vigilantní prvky v podobě trestání „hříšníků“ zviditelněním, není to ale jediný cíl tvůrců, tím dalším může být i osvěta uživatelů, poukázání na problémy řidičů a chodců na silnicích, ale zejména jde o zábavu a nalákání uživatelů na vlastní tvorbu.

Tato videa jsou nejenže lidmi tolerována, ale záměrně vyhledávána. V komentářích lidé neodsuzují nikdy tvůrce, ale chování účastníku silničního provozu.

Nutné je zmínit, že napříč sociálními sítěmi nalezneme nespočet obsahu s obdobnou tématikou nejen ze silnic. Populární jsou videa konfliktů lidí, videa obsahující názvy „karma“ nebo „instant karma“, ve kterých jedinec udělá nějakou schválnost druhému, která se mu nevydaří a on sám na jednání nějakým způsobem doplatí, ale nemusí se jednat pouze o schválnost nebo škodolibost, ale předmětem může být právě protiprávní jednání, různé nevydařené krádeže nebo fyzické napadání druhého, které se agresorovi nevydaří.

Rizika: U podobného obsahu na internetu víceméně hrozí zveřejnění osobních údajů, které mohou vést k identifikaci konkrétní osoby případně osob. Dalším rizikem je i převzetí záznamu nebo jeho části veřejnoprávním médiem, což se běžně děje a oběti, resp. člověku dopouštějícího se přestupku (případně nějaké morální normy), se dostane mnohem větší pozornosti. I v tomto případě může hrozit výskyt dalších doprovodných jevů jako je doxing a následná šikana oběti, zejména v případech, kdy oběť nějakým způsobem ve videu vyniká (jeho jednání je uživateli shledáno jako mnohem závažnější nebo je nějakým způsobem vyzdviženo, je mu dán největší prostor).

Následky: Ve většině případů nemá velký vliv na dotčené osoby (rozhodně výrazně menší než v případech lovců pedofilů). Videím se nedá upřít osvěta lidí v podobě nesprávného příkladu a pobavení uživatelů.

2.5 Seznamy nepoctivců

Samostatnou kapitolou určitého druhu digilantismu jsou webové stránky, vytvořené komunity na sociálních sítích sdílející seznam podvodníků na internetu. Jako příklad může posloužit web podvodnabazaru.cz, kam může běžný uživatel internetu nahlásit podvodníka zadáním jeho identifikátorů číslo jeho účtu, variabilní symbol, telefonní číslo, e-mail a popis podvodu. Webová stránka je dostupná od roku 2020 a je stále funkční. Lze v ní vyhledávat podle čísla účtu shora uvedených identifikátorů, stránka má i část se statistikou. Na sociální síti Facebook je nespočet skupin s touto problematikou, namátkou např. skupiny

s názvem: Podvodníci z marketplace aj., Podvodníci z Sbazaru, Bazoše, aj., FB zloději a podvodníci – ohlašovna, aj., některé skupiny jsou zaměřeny mnohem konkrétněji např. na fototechniku – Foto (Ne)poctivci. Smyslem všech skupin je sdílet informace o podvodnících, aby se případní další kupující nebo prodávající nestali obětí podvodu. Mnohdy jsou ovšem ve skupinách zveřejňovány osobní údaje podvodníků včetně jejich fotografií.

Rizika: Rizikem může být vyhledávání podvodníka, jeho veřejné lynčování, a to nejen v síti Internet ze strany rozhněvaných podvedených lidí. Dalším vcelku výrazným rizikem může být zapsání údajů podvedeného člověka. V současnosti mezi podvodníky funguje trend tzv. „podvodného bankéře“, který přiměje lidi investovat do kryptoměn, avšak jen domněle, lidé neinvestují, ale jednoduše řečeno přeposílají peníze podvodníkům i prostřednictvím jiných podvedených osob a vzniká tak reálné riziko, že číslo účtu podvedené osoby se objeví v těchto databázích jako číslo účtu podvodníka. (nemusí se jednat pouze o „podvodného bankéře“, ale i o případy RIP podvodů – reverzních inzertních podvodů). Dokonce i některá telefonní čísla mohou být skutečnými pachateli podvržena (spoofing) a ta zanesena do databází digilantistů, ačkoli patří osobám, které se ničím neprovinili a nemají o protiprávním jednání tušení.

Následky: Zveřejnění osobních údajů lidí a s tím spojený zásah do jejich soukromí ať už se jedná a skutečné podvodníky či nikoli. Určitým způsobem může lidem posloužit vyvarování se prodeje či nákupu se osobou, která se podvodů skutečně dopouští.

2.6 Prezidentské volby 2023

Možná ne přímo počin digilantistů bylo vytvoření falešných webových stránek jednoho z kandidátů na prezidenta České republiky před druhým kolem prezidentských voleb. Doména generalpavel2023.com je v současné době nedostupná, avšak díky webovému nástroji Wayback Machine pořizující snímky webových stránek, se lze i dnes podívat, jak stránka vypadala a jaké přinášela informace v době, kdy byla v konkrétním čase zachycena služnou Wayback Machine. Služba tuto stránku archivovala 5x, a to v období 22. ledna 2023 do 26. ledna 2023. I z web archivu služby Wayback Machine je na první pohled zřejmé, že se jedná o velmi zdařilou kopii originálních webových stránek Petra Pavla. Pro

přesnost lze zmínit, že originální stránky mají doménu generalpavel.cz. Těsně před druhým kolem prezidentských voleb byl pro české uživatele internetu k dispozici tento nový falešný web, který přinášel informaci o náhlé smrti generála Pavla ve čtvrtek v ranních hodinách dne 26.1.2023, konkrétně bylo na webu zveřejněno následující:

„*PETR PAVEL (1. 11. 1961 - 26. 01. 2023)*

Tým kandidáta na prezidenta České republiky Petra Pavla vyjadřuje upřímnou soustrast rodině, blízkým a kolegům generála Petra Pavla, který brzo ráno ve čtvrtek 26. ledna 2023 náhle zemřel.

Petr Pavel (1. listopadu 1961 - 26. ledna 2023) byl český voják, armádní generál Armády České republiky ve výslužbě. V letech 2012–2015 byl náčelníkem Generálního štábu Armády České republiky. Mezi roky 2015 a 2018 působil ve funkci předsedy vojenského výboru NATO a stal se tak prvním zástupcem zemí bývalé Varšavské smlouvy, který nastoupil do nejvyšší vojenské funkce Severoatlantické aliance NATO.

Dne 6. září 2022 oficiálně oznámil kandidaturu na prezidenta České republiky ve volbách v roce 2023. Se ziskem 35,40 % hlasů vyhrál první kolo a tím postoupil do druhého finálového kola prezidentských voleb.“[39]

Dezinformace okamžitě zaplavila internet, šířila se napříč sociálními sítěmi, reagovala na ní veškerá media, televize, rozhlasové vysílání, zpravodajské weby. Falešnou webovou stránku doprovázel i e-mail s odkazem na ní, který byl zasílán nezjištěnému počtu osob v České republice. E-maily byly rozesílány z ruského serveru Yandex a nebylo překvapením, že webová stránka byla vytvořena tak, aby její tvůrci nebyli snadno dohledatelní. Doména byla vytvořená na anonymních serverech, za které se platí kryptoměnami a tvůrci o sobě nezanechávají žádné osobní údaje (nebo zanechávají smyšlené).[40]

[39] Generalpavel2023.com. In: *Wayback arMachine* [online]. 2023. [cit. 27.1.2023]. Dostupné z: https://web.archive.org/web/20230126094350/https://generalpavel2023.com/

[40] Kopie Pavlova webu pochází z anonymního serveru, e-mailové adresy z ruského Yandexu. In: *iROZHLAS – spolehlivé zprávy* [online]. 2023 [cit. 27.1.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/petr-pavel-volebni-web-anonymni-server-falesna-zprava_2301261442_pik

Cílem práce není posoudit ani hodnotit na kolik se jednalo o předvolební boj, jaká byla motivace tvůrců webové stránky, ale pouze poukázat na možnost spojenou s vigilantismem v kyberprostoru.

I díky relativně čerstvému typu útoku nelze nyní s jistotou říct, zda jde o počin digilantistů či nikoli, v tom je spatřováno jedno z rizik. V některých případech lze digilantní jednání identifikovat až s odstupem času, po získání většího množství informací nebo např. po tom, co se k jednání digilantisté sami přihlásí. Sama skutečnost, zda se jedná o vigilantní chování v kyberprostoru či nikoli je v době prováděného útoku možná irelevantní, ale jedná se o nezbytnou kriminalistickou otázku, která by měla být při šetření činu zodpovězena (kdo za jednáním stojí a proč se ho dopustil, jaký měl motiv).

Pokud zůstaneme u prezidentských voleb a tehdejšího kandidáta Petra Pavla, nalezeno bylo i dezinformační video, které se v průběhu voleb šířilo sociálními sítěmi. V sestříhané a upravené verzi videa Pavel říká: *„…jediná možnost, jak dovést situaci do zdárného konce, je pomoct Ukrajině tu válku vyhrát a my to můžeme udělat z naší strany právě tím, že vstoupíme do války s Ruskem*.“. Na originálním zvukovém záznamu je patrné, že Pavel říká vlastně pravý opak: „*No, ono to nejde takto udělat. Protože kdybychom to takto udělali, tak vstoupíme do války s Ruskem, a to by bylo mnohem horší. Takže jediná možnost, jak dovést situaci do zdárného konce, je pomoct Ukrajině tu válku vyhrát. A my to můžeme udělat z naší strany tím, že ji dodáme kvalitnější zbraně, že budeme pokračovat v sankcích proti Rusku, protože přímo do toho vstoupit opravdu nemůžeme*.“[41]

Je otázkou na kolik podobné dezinformace skutečně ovlivnily volby, jisté ovšem je, že právě ze strachu zapojení České republiky do války ovlivnilo minimálně menšiny v mosteckém Chánově. Naprostá většina obyvatel jsou zde Rómové a ti nejen že se postarali o rekordní účast u prezidentských voleb, ale právě ze strachu z války volili druhého z kandidátů, Andreje Babiše.[42]

[41] ŽABKA, Jan. Zmanipulované video s Pavlem: „Vstoupíme do války s Ruskem.“. In: *HlídacíPes.org* [online]. 2023 [cit. 27.1.2023]. Dostupné z: https://hlidacipes.org/zmanipulovane-video-s-pavlem-vstoupime-do-valky-s-ruskem/

[42] VANŽURA, Alexandr, VOKURKA, Martin. Vyloučené lokality Ústeckého kraje volily Babiše, lidé z nich se bojí války. In: *Deník.cz.* [online] 2023 [cit. 2.2.2023]. Dostupné z: https://teplicky.denik.cz/zpravy_region/vyloucene-lokality-ustecky-kraj-babis-volby-prezident.html

Rizika: Šíření dezinformací je v dobách, kdy drtivá většina obyvatelstva má mobilní zařízení a pravidelně jím navštěvuje kyberprostor, je jedna z nejefektivnějších zbraní vůbec. Dnes se lidé spoléhají na informace, které vyhledají nebo se jim sami nabídnou k zobrazení na internetu, někteří jedinci si informace neověřují, buď nechtějí, nevědí kde anebo vůbec netuší, že se můžou stát obětí falešných informací. Dnes je navíc informací tolik, že jsme jimi zahlceni a je opravdu těžké si udržet zdravý úsudek a v některých případech zhodnotit pravdivost tvrzení v kyberprostoru. Druhým nastíněným rizikem je pak občasná nemožnost identifikovat vigilantismus v kyberprostoru ihned.

Následky: Pokud dopady vztáhneme čistě na tento konkrétní případ, je možné ovlivnění voleb, či volební účasti. Díky dezinformacím někteří obyvatelé mohou ze strachu nebo na základě nepravdivých informací volit stranu, kterou by jinak nevolili. Je zcela jasné, že obětí nebyl pouze Petr Pavel, ale podobné falešné zprávy jsou součástí každých voleb a obětí dezinformací tak byl i Andrej Babiš v nějaké formě. Pokud ovšem hovoříme o obětech dezinformací jsou jimi také samotní voliči, nejen kandidáti.

2.7 VKontakte

V průběhu víkendu 19. - 20.3.2022 hnutí Anonymous proniklo do ruské sociální sítě v VKontakte (vk.com, což je obdoba populární sociální sítě Facebook). 12 milionům uživatelů tak obdrželo v ruském jazyce zprávu o skutečném dění na Ukrajině, o bombardování civilních cílů, o počtu mrtvých na obou stranách, o tom, že se jedná o okupaci, nikoli o „speciální vojenskou operaci“ jak Rusko informuje svůj lid. Mnoho z uživatelů zprávu sdíleno a přeposílalo dalším uživatelům.[43]

Několik dní před napadením sociální sítě VKonte se podařilo hnutí Anonymous získat i 820 GB dat z ruského úřadu Roskomnadzor (úřad pro monitorování, kontrolu a cenzuru médií). 363 994 dokumentů zveřejnili na serveru DDoSecrets (obdoba WikiLeaks).[44]

[43] INDROVÁ, Monika. Anonymous napadli ruskou síť VKontakte, uživatelům ukázali pravdu o invazi. In: *iDNES.cz* [online]. 2022 [cit. 28.1.2023]. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/anonymous-rusko-hackeri-utok-valka-na-ukrajine.A220322_104037_zahranicni_indr

[44] HRON, Jan. Anonymous napadli ruský cenzurní úřad, zveřejnili 360 tisíc dokumentů. In: *iNDES.cz.* [online] 2022 [cit. 28.1.2023]. Dostupné z:

Od počátku války Ukrajiny s Ruskem hnutí Anonymous podniklo i další kyberútoky vůči Rusku, napadají vládní servery, ruská media, kde vysílají necenzurované záběry z války případě pouští ukrajinskou hymnu.
K hnutí se připojilo i další hackerské uskupení Squad303, které na webových stránkách 1920.in zveřejňují krátké prohlášení a nabízejí komukoli umožnit zaslat textovou zprávu náhodně vybranému ruskému občanovi prostřednictvím SMS, aplikace jako je WhatsApp, Viber, Telegram, ale také prostřednictvím e-mailu či volání.[45]

Rizika: Objektivním pohledem na věc je zřejmé, že hnutí Anonymous naplňuje znaky některých skutkových podstat trestných činů. S výjimkou Ruska a občanů vyjadřujícím podporu Ruska, toto jednání není odsuzováno a žádným jiným státem řešeno (ve smyslu trestního stíhání). Mlčky je akceptováno, pro jednu válečnou stranu je žádoucí dle pořekadla „nepřítel mého nepřítele, je můj přítel“. Rizikem je pak jednání takovýchto hackerských skupin vůči ostatním. Lze si představit i situaci útoků (nijak ojedinělých) na zdravotnická zařízení, což může ohrozit zdraví a životy osob zcela nevinných. Hrozí zde vcelku velké riziko kyberterorismu, nejen ze strany Anonymous vůči Rusku, ale obecně v případě takto vyhroceného konfliktu ze strany podporovatelů obou znepřátelených stran. Příliš mnoho věcí je dnes připojeno do sítě Internet a řízeno elektronicky se zabezpečením, které je možné překonat, není těžké si představit odpojení cílů od elektřiny, provádění změn v navigačních systémech, instalace škodlivých softwarů do kteréhokoli systému atp.
Následky: Ačkoli byla nalezena tvrzení, že většina útoků Anonymous na Ruské cíle je jako „házení vajec na tank“[46] nelze s takovýmto tvrzením zcela souhlasit. Při srovnání boje skutečných vojáků, kteří jsou v ohrožení vlastního života je kyberútok relativně bezpečnou formou boje, souhlasím tedy s tvrzením, že

https://www.idnes.cz/zpravy/zahranicni/anonymous-rusko-ukrajina-hackeri-dokumenty-cenzura-roskomnadzor.A220311_084906_zahranicni_jhr
[45] SQUAD303. We the people of the world have a message to the Russian nation. In: *1920.in.* [online] 2023 [cit. 29.1.2023]. Dostupné z: https://1920.in
[46] ZELENKA, Filip. Většina útoků Anonymous na Rusko je jako házení vajec na tank, říká etický hacker. In: *e15.cz* [online]. 2022 [cit. 29.1.2023]. Dostupné z: https://www.e15.cz/rozhovory/vetsina-utoku-anonymous-na-rusko-je-jako-hazeni-vajec-na-tank-rika-eticky-hacker-1388313

„skutečná válka je horší než kybernetická“.[47] Ovšem i kybernetické útoky mohou přinést vcelku významné výsledky. V případě takových útoků může upadat morálka vojáků, civilistů i velitelů. Mohou dále přinést strategické informace o budoucích taktikách nepřátelské země, rozmístění strategických cílů a další relevantní informace. Minimálně je hnutí Anonymous a jim podobní obrovská morální podpora.

2.8 Pátrání Policie České republiky

Policie České republiky jde s dobou nebo se snaží udržet krok s vývojem kyberprostoru a má založené účty na sociální síti Facebook, Instagram, Twitter, Youtube, samozřejmostí jsou i funkční webové stránky. Na sociálních sítích, webu nebo prostřednictvím sdělovacích prostředků často pátrá po osobách, věcech a obrací se k veřejnosti s prosbou o pomoc. I takováto prosba může být živnou půdou pro vigilantisty v kyberprostoru. Ti v těchto případech mohou být velmi nápomocní policii při pátrání.

Rizika: I zde hrozí možnost závadových jednání v kyberprostoru, z prosté pomoci policii se vyhledávaný může stát obětí doxingu, kyberšikany, a to zejména v případech, které ve společnosti nějakým způsobem rezonují, v lidech vzbuzující emoce. Proto je zejména na policii žádosti o pomoc formulovat co nejlépe, aby se podobným nežádoucím jevům dalo zabránit.

Následky: Většinou jsou dopady spíše příznivější a žádosti o pomoc pomáhají policii nalézt osoby, věci, vozidla a přispívat tak k objasnění trestné činnosti. Pokud by tomu tak nebylo, zcela jistě by tyto metody policie nepoužívala.

[47] ZELENKA, Filip. Většina útoků Anonymous na Rusko je jako házení vajec na tank, říká etický hacker. In: *e15.cz* [online]. 2022 [cit. 29.1.2023]. Dostupné z: https://www.e15.cz/rozhovory/vetsina-utoku-anonymous-na-rusko-je-jako-hazeni-vajec-na-tank-rika-eticky-hacker-1388313

Závěr

Vigilantismus v kyberprostoru je fenomén, který tu bude i nadále a s vývojem moderních technologií a kyberprostoru se bude jistě dále vyvíjet. V současné době nastupuje trend umělé inteligence (př. ChatGPT, Dall-E), která je schopna se učit, po zadání krátkých výstižných příkazů dokáže nakreslit obrázky, dokáže opravit chyby ve zdrojových kódech nebo například i napsat bakalářskou práci na zvolené téma (zatím pouze v angličtině). V tom spatřuji budoucnost vigilantismu, bude tak i pro jedince neznalého softwaru snadné vytvořit škodlivý software, zaútočit na servery nebo jen nalézt konkrétní osobu v síti, s tím vším v budoucnu může pomoci umělá inteligence.

Digilantistou se může stát každý člověk vlastnící mobilní zařízení připojené do sítě Internet. Na základě vyhledaných příkladů je zřejmé, že takovým osobám je poskytována anonymita, dříve možná jen domnělá, ale dnes v době, kdy si každý může jednoduše aktivovat nějaký nástroj na anonymizaci svého skutečného umístění v síti, je anonymita reálná navíc umocněná tím počtem spolupracujících digilantistů. Pokud se na útoku, vyhledávání, šikanování bude podílet desítky tisíc lidí, není v současné době možné a v silách policie všechny tyto osoby identifikovat. Ztěžuje to například fakt, který poskytovatelům určuje dobu, po kterou mají být data uchována. Pro upřesnění jen zmíním, že u některých forem může být digilantistou každý, ale při některých sofistikovanějších útocích (průniky do počítačových systémů, tvoření škodlivého softwaru atp.) je nezbytná odborná znalost hardwaru a softwaru.

Digilantismus je rozhodně velice komplikovanou záležitostí především ve vztahu k orgánům činným v trestním řízení, které se mnohdy snaží suplovat. Nedá se říci, že digilantismus je pouze škodlivým jevem, určitě může pomáhat společnosti, policii při pátrání po osobách a věcech, v případech, kdy jsou informace o protiprávním jednání předávány policii, digilantismus může působit i preventivně, poučně, zábavně, ale samozřejmě také protiprávně. Troufám si tvrdit, že v některých případech je digilantismus dokonce žádoucí, jako například nyní při podpoře Ukrajiny ve válce. Ta pomyslná hranice, na které se vigilantismus nachází je velice tenká.

Hlavní riziko spatřuji, ačkoli to z praktických příkladů přímo nevyplývá, v možném vzniku extremismu nebo přímo terorismu, a to nejen v kyberprostoru, dále pak absenci presumpce neviny a trestání obětí tak, jak digilantisté uznají za vhodné, ve většině případů zcela neadekvátně situaci, a ne v souladu se zákony, o trestu, vině a nevině může rozhodnout pouze soud. Dalším rizikem je zapojení se do útoků obrovského množství lidí, což z něho téměř vždy učiní útok neodvratitelný, v některých případech hrozí nejen veliká finanční újma, ale i újma na zdraví nebo životě.

Následky vigilantismu mohou být také různé, od prostého humoru, přes nemorální jednání, protiprávní jednání ve formě přestupků, trestných činů, ale i následky velmi závažné s obrovskými finančními škodami či dokonce újmou na životech.

Jedná se o fenomén s obrovským dosahem, práce je jen malým exkurzem do problematiky. Množství lidí si počíná jako vigilant v kyberprostoru, aniž si uvědomuje, že jím je.

Protiprávní jednání vigilantů, v případě, že se nějakého dopouštějí, je z pohledu trestního zákoníku, velice snadno kvalifikovatelné, výjimku donedávna tvořily pouze DDoS útoky, ale i ty jsou po úpravě trestního zákoníku bezproblémové. Problém spatřuji spíše v identifikaci konkrétního pachatele, kterému síť Internet poskytuje anonymitu a v případě používání nástrojů sloužících k maskování skutečného umístění v síti Internet je tak jeho nalezení extrémně obtížné (nikoli však nemožné).

I když se může jevit tento fenomén v některých případech užitečným a bezesporu užitečným někdy je to fenomén nebezpečný.

Seznam použité literatury

KOLOUCH, Jan. *Cybercrime.* 1. Praha: CZ.NIC, 2016. ISBN *978-80-88168-18-8.*

KOLOUCH, Jan, BAŠTA, Pavel, KROPÁČOVÁ, Andrea, KUNC, Martin. *CyberSecurity.* 1. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

SMEJKAL, Vladimír. *Kybernetická kriminalita.* 1. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-502-2.

DRMOLA, Jakub. *Protidžihádský vigilantismus v kyberprostoru.* 1. *Brno: EDIS, 2018, ISBN: 978-80-210-8985-3.*

Gibson, William. *Neuromancer*, Plzeň: Laser – books, 1998. ISBN 80-7193-048-2.

OLSON, Parmy. J*sme Anonymous,* Praha: Práh, 2012, ISBN 978-80-7252-400-6.

VEGRICHTOVÁ, Barbora. *Extremismus a společnost*. 2. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-665-1.

VEGRICHTOVÁ, Barbora. *Hrozba radikalizace*. Praha: Grada, 2017. ISBN 978-80-271-2031-4.

Zákon č. 89/2012 Sb., Zákon občanský zákoník. In: Zákony pro lidi [online]. © AION CS, 2010-2022 [cit. 2.12.2022]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2012-89.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Zákony pro lidi [online]. © AION CS, 2010-2022 [cit. 2.12.2022]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2014-181.

Zákon č. 40/2009 Sb., Trestní zákoník. In: *Zákony pro lidi* [online]. © AION CS, 2010-2023 [cit. 25.1.2023]. Dostupný také z: https://www.zakonyprolidi.cz/cs/2009-40.

Sdělení č. 104/2013 Sb. m.s., *Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě*. In: Zákony pro lidi [online]. © AION CS, 2010-2023 [cit. 25.1.2023]. Dostupný také z: https://www.zakonyprolidi.cz/ms/2013-104.

ČESKÝ STATISTICKÝ ÚŘAD [ČSÚ]. *Internet zrychluje a přesouvá se na chytré telefony*, In: *Český statistický úřad* [online]. Praha, *2022, [cit. 1.12.2022,]* dostupné z: https://www.czso.cz/csu/czso/internet-zrychluje-a-presouva-se-na-chytre-telefony.

ČESKÝ STATISTICKÝ ÚŘAD [ČSÚ]. *Počítače a internet v domácnostech. In: Český statistický úřad* [online]. Praha, *2022 [cit. 1.12.2022]* dostupné z: https://www.czso.cz/documents/10180/164606768/0620042201.pdf/5699654d-a722-44c9-a5e8-80443c89be18?version=1.1.

JOHNSTON, Les. *What is vigilantism?,* In: Oxford University Press, [online]. Velká Británie, 1996, [cit. 3.12.2022]. Dostupné z: https://doi.org/10.1093/oxfordjournals.bjc.a014083.

TROTTIER, Daniel. *Digital Vigilantism as Weaponisation of Visibility, In: Springer Nature Switzerland [online]. Švýcarsko, 2017 [cit. 4.12.2022],* Dostupné z: https://link.springer.com/article/10.1007/s13347-016-0216-4.

KARATZOGIANNI, Athina. Anonymous hackers could be Islamic State's online nemesis*,* In: *The Conversation.com* [online]. 2015, [cit 6.12.2022]. Dostupné z: https://theconversation.com/anonymous-hackers-could-be-islamic-states-online-nemesis-50876.

BESSER, Vilém. Kdo jsou vlastně vlivní hackeři Anonymous, kteří děsí svět. In: *Forum24* [online]. 2015 [cit. 6.12.2022]. Dostupné z: https://www.forum24.cz/kdo-jsou-vlastne-vlivni-hackeri-anonymous-kteri-desi-svet/.

GREGORY, Jennifer. 10 Years Later, What Did LulzSec Mean for Cybersecurity?. In: *Security Intelligence* [online]. © 2022 IBM [cit. 6.12.2022]. Dostupné z: https://securityintelligence.com/articles/lulzsec-10-years-later-cybersecurity-influence-meaning/.

Leading Member of the International Cyber Criminal Group LulzSec Sentenced in Manhattan Federal Court. In: *FBI Federal Bureau of Investigation* [online]. 2014 [cit. 6.12.2022]. Dostupné z: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/leading-member-of-the-international-cyber-criminal-group-lulzsec-sentenced-in-manhattan-federal-court.

VODRÁŽKA, Prokop. Rusové bojují proti agresivním řidičům. Podpořil je i Putin. *In: Aktuálně.cz [online]. 2015 [cit. 7.12.2022]. Dostupné z: https://magazin.aktualne.cz/rusove-bojuji-proti-agresivnim-ridicum-podporil-je-i-putin/r~bcc4cb761f3611e58a300025900fea04/.*

What is WikiLeaks. In: *WikiLeaks* [online]. 2015 [cit. 7.12.2022]. Dostupné z: https://wikileaks.org/What-is-WikiLeaks.html.

SOBOLA, Ondřej. Před 10 lety server WikiLeaks zveřejnil utajované vojenské dokumenty o válce v Iráku, Assange teď čeká na soud o vydání do USA. In: *Česká televize* [online]. 2020 [cit. 7.12.2022]. Dostupné z: https://ct24.ceskatelevize.cz/svet/3212524-pred-10-lety-server-wikileaks-zverejnil-utajovane-vojenske-dokumenty-o-valce-v-iraku.

CUMMINGS, William. Six big leaks from Julian Assange's WikiLeaks over the years. In: *USA Today News* [online]. 2019 [cit. 7.12.2022]. USA. Dostupné z: https://eu.usatoday.com/story/news/politics/2019/04/11/julian-assange-six-wikileaks-most-memorable-revelations/3434371002/.

DOWNEY Tom. China's Cyberposse, In: *The New York Times Magazine* [online]. New York, 2010 [cit. 8.12.2022]. Dostupné z: https://www.nytimes.com/2010/03/07/magazine/07Human-t.html.

HATTON, Celia. China's internet vigilantes and the 'human flesh search engine'. In: *BBC* [online], Peking, 2014 [cit. 9.12.202]. Dostupné z: https://www.bbc.com/news/magazine-25913472.

About Us. In: WaybackMachine [online]. 2013 [cit.10.12.2022]. Dostupné z: https://web.archive.org/web/20130417180227/http://letzgohunting.com/view_page.php?pid=1.

Letzgo Hunting denies blame for man's suicide. In: *BBC* [online]. 2013 [cit. 11.12.2022]. Dostupné z: https://www.bbc.com/news/uk-england-leicestershire-24145142.

O čem je film V SÍTI. In: *Dokument V síti* [online]. [cit. 11.12.2022]. Dostupné z: https://vsitifilm.cz/jsem-rodic.html.

Policie kvůli dokumentu V síti vyšetřuje sexuální predátory. Jeden už od soudu odešel s trestem. In: *iROZHLAS - spolehlivé zprávy* [online]. 1997-2022 [cit. 23.1.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/v-siti-dokument-film-vit-klusak-barbora-chalupova-policie-podezreli_2002181141_dok.

PHILLIPS, Tom. Five years ago today, Sony admitted the great PSN hack. In: *Eurogamer* [online]. 2016, [cit. 24.1.2023]. Dostupné z: https://www.eurogamer.net/sony-admitted-the-great-psn-hack-five-years-ago-today.

RICHWINE, Lisa. Cyber attack could cost Sony studio as much as $100 million. In: Reuters [online]. 2014 [cit. 24.1.2023]. Dostupné z:

https://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209.

NICHOLSON, Paul. Five Most Famous DDoS Attacks and Then Some. In: *A10 Networks* [online]. 2022 [cit. 24.1.2023]. Dostupné z: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

DDoS útok. In: *Eset* [online]. Praha, 1992-2023 [cit. 24.1.2023]. Dostupné z: https://www.eset.com/cz/ddos-utok/.

Generalpavel2023.com. In: *WaybackMachine* [online]. 2023. [cit. 27.1.2023]. Dostupné z: https://web.archive.org/web/20230126094350/https://generalpavel2023.com/.

Kopie Pavlova webu pochází z anonymního serveru, e-mailové adresy z ruského Yandexu. In: *iROZHLAS – spolehlivé zprávy* [online]. 2023 [cit. 27.1.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/petr-pavel-volebni-web-anonymni-server-falesna-zprava_2301261442_pik.

ŽABKA, Jan. Zmanipulované video s Pavlem: „Vstoupíme do války s Ruskem.“. In: *HlídacíPes*.org [online]. 2023 [cit. 27.1.2023]. Dostupné z: https://hlidacipes.org/zmanipulovane-video-s-pavlem-vstoupime-do-valky-s-ruskem/.

VANŽURA, Alexandr, VOKURKA, Martin. Vyloučené lokality Ústeckého kraje volily Babiše, lidé z nich se bojí války. In: *Deník.cz.* [online] 2023 [cit. 2.2.2023]. Dostupné z: https://teplicky.denik.cz/zpravy_region/vyloucene-lokality-ustecky-kraj-babis-volby-prezident.html.

INDROVÁ, Monika. Anonymous napadli ruskou síť VKontakte, uživatelům ukázali pravdu o invazi. In: *iDNES.cz* [online]. 2022 [cit. 28.1.2023]. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/anonymous-rusko-hackeri-utok-valka-na-ukrajine.A220322_104037_zahranicni_indr.

HRON, Jan. Anonymous napadli ruský cenzurní úřad, zveřejnili 360 tisíc dokumentů. In: *iNDES.cz.* [online] 2022 [cit. 28.1.2023]. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/anonymous-rusko-ukrajina-hackeri-dokumenty-cenzura-roskomnadzor.A220311_084906_zahranicni_jhr.

SQUAD303. We the people of the world have a message to the Russian nation. In: *1920.in.* [online] 2023 [cit. 29.1.2023]. Dostupné z: https://1920.in.

ZELENKA, Filip. Většina útoků Anonymous na Rusko je jako házení vajec na tank, říká etický hacker. In: *e15.cz* [online]. 2022 [cit. 29.1.2023]. Dostupné z: https://www.e15.cz/rozhovory/vetsina-utoku-anonymous-na-rusko-je-jako-hazeni-vajec-na-tank-rika-eticky-hacker-1388313.

Crowdsourcing. In: SCS.ABC.CZ [online]. Česká republika: 2005-2022 [cit. 5.12.2022]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/crowdsourcing.

We Are Legion: The Story of the Hacktivists [dokument]. Režie Brian Knappenberger. USA/Velká Británie. 2012.

Don't F**k with Cats: Hunting an Internet Killer [dokument]. Režie Mark Lewis. Velká Británie. 2019.