POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminologie

Kyberprostor jako prostředí pro páchání trestné činnosti – kriminologická analýza

Bakalářská práce

Cyberspace as an environment for crime – criminological analysis

Bachelor thesis

VEDOUCÍ PRÁCE

PhDr. Marešová Alena Ph.D.

AUTOR PRÁCE

Myroslava Dzobak

PRAHA
2023

Čestné prohlášení

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

V Praze, dne……

……

Myroslava Dzobak

Anotace

Bakalářská práce na téma „Kyberprostor jako prostředí pro páchání trestné činnosti – kriminologická analýza“. V prvních třech kapitolách se věnuji fenoménu a podstatě kyberkriminality a také kyberkriminologii. Následující kapitoly se věnují kyberkriminalitě a jejím druhům v rámci kyberprostoru a kriminologické analýze kyberzločince. V závěru práce jsou shrnuty hlavní problematické otázky, které potřebují postupné řešení.

Klíčová slova

Kyberprostor, kybernetický útok, kybernetická kriminalita, kyberzločinci, hacking.

Annotation

Bachelor thesis on the topic of "Cyberspace as an Environment for Committing Crime: a Criminological Analysis". The first three chapters deal with the phenomenon and nature of cybercrime and cybercriminology. The following chapters are devoted to cybercrime and its types within cyberspace and to criminological analysis of the cybercriminal. The thesis concludes with a summary of the main issues that need to be gradually solved.

Keywords

Cyberspace, cyberattack, cybercrime, cybercriminal, hacking.

Obsah

Úvod

Digitální technologie jsou nedílnou součástí našeho každodenního života. Ať už máme doma počítač, využíváme digitální služby státní správy a samosprávy nebo jen využíváme elektronické zařízení, závislost společnosti na technologiích neustále roste. Bezpečné digitální prostředí především zvyšuje důvěru veřejnosti a přispívá ke stabilitě a prosperitě státu. Vláda a podnikatelská sféra rovněž využívají příležitostí technologické revoluce prostřednictvím většího zavádění a používání digitálních technologií. Existuje ale i špatná stránka, a to trestná činnost. Organizované zločinecké skupiny se začínají přesouvat do kyberprostoru a neustále se rozrůstají. Kyberkriminalita se vyvíjí neuvěřitelně rychle a neustále se objevují nové druhy trestné činnosti. Proto musíme držet krok s digitálními technologiemi, chápat příležitosti, které vytvářejí pro kyberzločince, a chápat, jak je lze využít jako nástroj boje proti kyberkriminalitě. Je nutné být opatrný a chovat se k jakýmkoliv zdrojům dat zodpovědně a opatrně. Rychlé pronikání digitálních technologií v posledních třech desetiletích způsobilo, že se do všech oblastí společnosti dostala zvláštní kategorie pachatelů, tzv. hackerů. Zločinecké skupiny hackerů jsou pro společnost velmi nebezpečné, protože když se dají dohromady, jsou schopny naplánovat silný kybernetický útok, a to i na zařízení kritické informační infrastruktury. Skupiny hackerů se také staly velmi reálnou hrozbou pro vlády, velké korporace a pro jednotlivce. Trend mazání hranic mezi hackerskými skupinami a organizovaným zločinem, který odborníci předpovídají již před několika let se stal skutečností. Ve skutečnosti můžeme dnes hovořit o vzniku nové formy organizovaného zločinu: hackerské komunity. Tyto okolnosti vyžadují vytvoření zvláštní normy, která by stanovila odpovědnost za organizování hackerské sítě a účast v ní. Taková norma by zajistila komplexní přístup k zabránění činnosti těchto zločineckých sítí a umožnila by adekvátní kriminalistické posouzení jednání osob vystupujících v roli organizátorů – koordinátorů hackerských organizací a podnikatelů.

Cíl práce

Cílem práce je shrnout současnou literaturu o kyberkriminalitě a poukázat na rozsah tohoto problému a navrhnout pomyslnou koncepci kriminologických teorií, které lze uplatnit pro posílení úsilí v oblasti vyšetřování a prosazování kyberkriminality. Kromě toho v práci se navrhuje zřízení akademického oboru „kybekriminologie“ na základě interdisciplinárního přístupu.

1. Kyberkriminalita – ohrožení veřejného informačního prostoru

1.1. Kyberkriminalita jako fenomén: předpoklady vzniku a rozvoje

Kriminologická literatura popisuje, že pojem kyberzločin byl formulován díky činnosti orgánů činných v trestním řízení vyspělých zemí Evropy a světa a odkazuje na trestné činy v oblasti počítačových informací a telekomunikací, nelegální oběh radioelektronické a speciální technické prostředky, distribuce licencovaného software zabezpečení počítačů, jakož i některé další druhy trestných činů.

Historie kyberkriminality je nedávný příběh, který se týká nás všech, problém kyberkriminality se dnes stal celosvětovým problémem.

Pojem kyberkriminalita se nyní často používá spolu s termínem počítačová kriminalita a tyto pojmy se často používají jako synonyma. Tyto pojmy jsou si velmi blízké, ale nejsou synonyma. Pojem cybercrime (v anglické verzi – *cybercrime*) je širší než „computer crime“ (počítačová kriminalita) a přesněji odráží povahu takového fenoménu, jako je kriminalita v informačním prostoru. Oxfordský slovník definuje předponu *„cyber“* jako součást složeného slova. Jeho význam je „týkající se informačních technologií, internetu, virtuální reality“.[1]

Podle Policie ČR pojem „*kybernetická kriminalita je odvozován od pojmu kybernetický prostor, případně zkráceně kyberprostor. Kyberprostor je virtuální prostředí, které nemá začátek a ani konec, nezná hranice států a nelze určit, jak rozsáhlý je. Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována Policií ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a*

[1] Oxford English Dictionary [online]. 20223 [cit.22-01-091.09]. Dostupné z: https: //www.oxfordlearnersdictionaries.com

komunikačních technologií jakožto významného prostředku k jejímu páchání (Policie ČR).“ [2]

Kyberkriminalita je tedy trestný čin související jak s používáním počítačů, tak s využíváním informačních technologií a globálních sítí. Pojem počítačová kriminalita přitom označuje pouze trestné činy spáchané na počítačích nebo počítačových datech.

Podle doporučení expertů OSN se pod pojmem kyberkriminalita skrývá jakýkoliv trestný čin, ke kterému může dojít pomocí počítačového systému nebo sítě v rámci počítačového systému.[3] Jakýkoli trestný čin spáchaný v elektronickém prostředí také může být klasifikován jako kyberkriminalita.

V současné době je kyberkriminalita rozsáhlým problémem a škodlivý software má za cíl nelegálně získat peníze. Rozvoj internetu je jedním z klíčových faktorů, které určují další narůstání tohoto problému. Firmy i jednotlivci si bez něj již nedokážou představit svůj život a stále více finančních transakcí probíhá online.

Kyberzločinci si uvědomili obrovské možnosti zisku prostřednictvím malwaru, který se objevil v posledních letech a mnoho dnešního malwaru je přizpůsobeno nebo prodáno jiným zločincům.

Úmluva Rady Evropy o kybernetické bezpečnosti specifikuje čtyři typy počítačových zločinů, které jsou definovány jako zločiny proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů:

- Nezákonný přístup – čl. 2 (neoprávněný přístup k celému počítačovému systému nebo jeho jakékoliv části);
- Nezákonný odposlech – čl. 3 (nezákonné úmyslné odposlechy

[2] Kyberkriminalita. Odbor prevence kriminality Ministerstva vnitra [online]. [cit. 2023–02–06]. Dostupné z: https://prevencekriminality.cz/prevence–kriminality/kyberkriminalita/

[3] United Nations Office on Drugs and Crime: The United Nations Congress on Crime Prevention and Criminal Justice [online]. 2021 [cit.2023-01-29]. Dostupné z: https://www.unodc.org/unodc/en/crimecongress/about.html

přenosů počítačových dat, která nejsou určena pro veřejnost, ~~do, z nebo~~ v rámci počítačového systému);

- Zasahování do dat – čl. 4 (nezákonné poškození, vymazání, porušení, změna nebo ukončení počítačových dat);
- Zásah do systému – čl. 5 (závažný protiprávní zásah do fungování počítačového systému zadáním, přenosem, poškozením, zničením, narušením, změnou nebo ukončením počítačových dat).
- Zneužívání zařízení – čl. 6 (schválení legislativní úpravy a jiná opatření, která budou k tomu nezbytná).[4]

Kromě transformace samotné kyberkriminality mění se i charakteristika hackera: původně to byli lidé se znalostmi a dovednostmi, kteří své jednání směřovali ani ne tak k nelegálním účelům jako spíše k hledání nových poznatků, dnes za kriminálními činy stojí kriminální byznys. Existuje dělení útočníků na osoby, které mají vysoké znalosti v této specifické oblasti, což lze přiřadit ke kategorii „Elita" a osoby, které dostaly do rukou hotový algoritmus, který zajišťuje provedení určitého pořadí akcí, přičemž mají velmi obecnou představu o procesech probíhajících v informačních systémech.

První kategorie kyberzločinců, kteří dnes představují největší hrozbu, má zcela charakteristické, výrazné rysy. Tyto zahrnují:

- schopnost páchat trestné činy anonymně, tajně;
- trestné činy se nejlépe páchají v podmínkách přeshraniční jurisdikce různých států;
- vysoké profesionální a intelektuální schopnosti hackera;
- možnost spojit různé počítače do jednoho mechanismu pro automatizované páchání trestné činnosti;
- absenci nebo dlouhou časovou prodlevu uvědomění si oběti, že je na ni spáchán trestný čin;

[4] Úmluva Rady Evropy č.185 o kybernetické kriminalitě ze dne 23.11.2001 [online]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104/zneni-20190705

- existenci velkého počtu obětí hackerského útoku;
- vyhnutí se přímému kontaktu s obětí svého protiprávního jednání.

První zmínka o použití počítače za účelem spáchání trestného činu byla zveřejněna v 60. letech 20. století. Po druhé světové válce v roce 1946 začalo několik společností využívat komerční počítače a v roce 1951 byl první komerční, sériově vyráběný počítač vyroben v USA. Na návrhu UNIVACu I pracovali hlavně J. Presper Eckert a John Mauchly, vynálezci ENIACu. V letech 1951 až 1958 bylo vyrobeno celkem 46 UNIVACů. Byly instalovány ve vládních institucích, soukromých korporacích a na třech amerických univerzitách. Počítače vyráběly hodně tepla, spotřebovávali však i hodně elektrické energie, byly objemné, drahé a nespolehlivé. Počítače první generace, postavené na elektronkách, měly nízkou rychlost a velmi nízkou spolehlivost.

V roce 1947 zaměstnanci americké společnosti „Bell" William Shockley, John Bardin a Walter Brettain vynalezli tranzistor. Tranzistory vykonávaly stejné funkce jako elektronické lampy, ale využívaly elektrické vlastnosti polovodičů. Ve srovnání s elektronkami jich tranzistory zabraly 200krát méně prostoru a spotřebovaly 100krát méně elektřiny. S vynálezem tranzistoru a použitím nových technologií pro ukládání dat do paměti bylo možné výrazně zmenšit velikost počítačů, zrychlit jejich funkci a zvýšit kapacitu paměti.

V roce 1954 oznámila společnost Texas Instruments zahájení hromadné výroby tranzistorů a v roce 1956 vytvořili vědci z Massachusetts Institute of Technology první počítač TX postavený výhradně na tranzistorech.[5]

V 60. letech minulého století se objevila třetí generace počítačů, ve kterých byly poprvé použity integrované obvody (mikroobvody). Zároveň se objevuje polovodičová paměť, která se dodnes používá v osobních počítačích jako RAM. V těchto letech získává výroba počítačů průmyslový rozměr. IBM jako první

[5] History: UNIVAC I. Census [online]. Eckert-Mauchly Laboratory in Philadelphia, PA, June 14, 1951 [cit. 2023-02-06]. Dostupné z: https://www.census.gov/history/www/innovations/technology/univac_i.html

implementovala rodinu počítačů – řadu plně kompatibilních počítačů od těch nejmenších, velikosti malé skříně (menší se tehdy nevyráběly) až po nejvýkonnější a nejdražší modely. Začátkem 60. let se objevily první minipočítače – malé počítače s nízkou spotřebou, cenově dostupné pro malé firmy nebo laboratoře. Minipočítače představovaly první krok na cestě k osobním počítačům, jejichž prototypy byly vydány teprve v polovině 70. let. Spolu s rychlým rozvojem v počítačové sféře začíná svůj rozvoj kybernetická kriminalita.

Počítačová kriminalita v 60. a 70. letech byla zcela jiná než kybernetická kriminalita v dnešní době. Tehdy nebyl internet a počítače nebyly připojeny k síti. V roce 1960 stál typický počítač několik milionů dolarů, zabíral prostor jedné místnosti a vyžadoval speciální klimatizační systém, aby počítač neshořel. Počítače mohl v té době využívat při své práci jen určitý okruh badatelů a vědců.

Druhá etapa rozvoje počítačových zločinů začíná v polovině 90. let minulého století bylo to období, kdy se internet šířil obrovskou rychlostí. Byla to doba kdy se osobní počítače a internet stávaly dostupnější pro všeobecné použití. V prosinci 1995 bylo odhadem 16 milionů registrovaných uživatelů internetu po celém světě a do května 2002 toto číslo vzrostlo na 580 milionů, téměř 10 procent celkové celosvětové populace (NUA, 2003). Je třeba poznamenat, že šíření internetu po celém světě bylo nerovnoměrné, například více než 95 procent z celkového počtu připojení k internetu se nacházelo ve Spojených státech, Kanadě, Evropě, Austrálii a Japonsku. V této době byl v historii trestných činů zaveden nový druh kriminality, který se nazýval „hacking“.

V počáteční fázi vývoje kybernetické kriminality je termín „hacking“ používán často, ale až později je hacking definován jako jeden z trestných činů zahrnutých do konceptu kybernetické kriminality. Právě hacking charakterizuje nezákonné jednání hackerů.

Kyberkriminalita je nejen technický a právní ale i společenský problém, jehož efektivní řešení vyžaduje především systematický přístup k rozvoji základů zajištění bezpečnosti životně důležitých zájmů občanů, společnosti a státu v kyberprostoru.

Podle mechanismů a způsobů páchání trestné činnosti v oblasti počítačové technologie má kyberkriminalita vysokou míru latence. Analyzované trestné činy mají velmi vysokou latenci, která podle různých údajů činí 85–90 %. Navíc skutečnosti odhalení nelegálního přístupu k informačním zdrojům ~~jsou~~ z 90 % mají náhodný charakter.

Tato data svědčí, že strážci zákona často jednoduše nevědí jak tyto trestné činy vyšetřovat a jak je u soudu dokazovat. Z toho plyne ztížení kvalitativně provádět vyšetřování těchto trestných činů, protože tradiční způsoby organizace a plánování vyšetřování v těchto podmínkách nefungují. Je nutné zvýšit efektivitu činnosti orgánů činných v trestním řízení, zvýšit úroveň nároků na úroveň profesionality strážců zákona, zvýšit efektivitu vyšetřování, zvýšit efektivitu a kvalitu jejich práce.

Dalším problémem, se kterým se vyšetřovatelé při vyšetřování počítačových trestných činů často potýkají je zjištění skutkové podstaty trestného činu. Je to dáno tím, že kyberzločiny jsou často spáchány v tzv. „kyberprostoru“, neznají hranice, velmi často jsou trestné činy páchány bez opuštění domova s pomocí osobního počítače. Kromě toho nelegální kopírování informací často zůstává nepovšimnuto, zavlečení viru do počítače bývá přičítáno neúmyslné chybě uživatele, který jej nedokázal „chytit“ při kontaktu s vnějším počítačovým světem. Také přístup obětí k trestnému činu spáchanému na nich není vždy adekvátní. Místo toho, aby oběti informovaly orgány činné v trestním řízení o nezákonném zásahu do počítačového systému, nespěchají s tím, protože se obávají poškození své obchodní či soukromé pověsti. Obvykle se jako oběti počítačových zločinů chovají lokální sítě, servery a fyzické osoby.

Je třeba zdůraznit, že profesionální kyberzločinci si za objekt své trestné činnosti vybírají místní sítě a servery velkých společností, „diletanti“ zase pronikají do informací počítačů jednotlivců a jen zřídka „hackují“ poskytovatele internetových služeb, zpravidla pro „bezplatný“ přístup k internetu.

Za pozornost stojí skutečnost, že poškozená strana, zastoupena velkými korporacemi, které systém vlastní, neochotně hlásí (pokud vůbec hlásí) orgánům

činným v trestním řízení skutek počítačové kriminality (napadení). Tím lze vysvětlit vysokou úroveň latence počítačových zločinů.

Kromě toho úředníci, mezi jejichž povinnosti patří zajišťování počítačové bezpečnosti, často nemají zájem o odhalení skutečnosti spáchání trestného činu. Přiznání faktu neoprávněného přístupu do systému pod jejich kontrolou zpochybňuje jejich odbornou kvalifikaci a selhání počítačových bezpečnostních opatření přijatých vedením může způsobit vážné vnitřní komplikace.

S efektivitou vyšetřování počítačových zločinů a jejich řešení před soudem souvisí i další problém. Jedná se o veřejné mínění, které počítačové zločiny nepovažuje za závažný trestný čin z toho důvodu, že počítačovým zločincům, když je vyšetřování ukončeno a je vydán soudní verdikt, jsou ukládány nízké tresty, nejčastěji – podmíněné. Odtud právní nihilismus, na jedné straně zločinci, kteří se cítí nepotrestání, a na druhé straně oběti, které se nechtějí obracet na orgány činné v trestním řízení s prohlášeními o neoprávněném přístupu, protože chápou, že zločinci nedostanou, podle jejich názoru, adekvátní trest.

V době globalizace a elektronické komunikace je tak jedním z nejpalčivějších problémů kybernetická bezpečnost. Lze rozlišit následující rysy fenoménu kyberkriminality, které ji charakterizují:

- rozsah hrozeb pro informační prostor není omezen na hranice jednoho státu;
- změny v kvantitativních a kvalitativních ukazatelích kyberkriminality, zejména prudký nárůst trestných činů počítačové profesionality a vysoké mobility u pachatelů této trestné činnosti;
- rozsah a úroveň kyberkriminality úzce souvisí s ekonomickou úrovní rozvoje společnosti v různých zemích a regionech;
- kybernetické hrozby se rychle mění a jsou technologicky stále vyspělejší;
- vysoká úroveň latence;
- závislost geografického rozložení na faktoru urbanizace.

Je třeba také poznamenat, že pro prevenci těchto trestných činů je zapotřebí dalšího výzkumu v těchto oblastech, mimo jiné v oblasti kriminologického výzkumu se zaměřit na zkoumání osobnostních vlastností kybernetických zločinců, zdokonalení tuzemské legislativy v oblasti ochrany státního tajemství a utajovaných informací, na mezinárodní spolupráci v oblasti informační bezpečnosti, zlepšení obsahu odborného vysokoškolského studia, zlepšení kvality informací a jejich ochrany. Vzdělávání specialistů v oblasti informační bezpečnosti státu atd..

1.2. Podstata a vlastnosti kyberkriminality

Rychlý rozvoj počítačových včetně internetových technologií jejich aktivní využívání ve všech sférách ekonomické činnosti se staly nejdůležitějším trendem ve vývoji moderní společnosti. Rostoucí využívání internetových technologií pro obchodování s cennými papíry, rozšíření elektronických plateb, internetový obchod, automatizace mnoha obchodních funkcí vytváří novou specifickou oblast trestné činnosti. V souvislosti s rostoucími procesy globalizace ve světě a informační společnosti se kyberkriminalita stala samostatným faktorem, který může ohrozit ekonomickou bezpečnost.

Aktivní zavádění informačních technologií do všech sfér činnosti vedlo ke změnám v seznamu hospodářské kriminality. Mezi tyto trestné činy začaly patřit počítačové trestné činy poškozující ekonomiku státu, jeho jednotlivá odvětví, podnikatelskou činnost, ale i ekonomické zájmy určitých skupin občanů.

Podle odhadů odborníků roční ztráty korporací z trestné činnosti v USA přesahují 200 miliard dolarů, z toho počítačových zločinů – 6 miliard dolarů. Velké Británii stojí počítačové zločiny 2 miliony liber ročně.[6]

Podle odhadu se každou sekundu na světě stane obětí kyberzločinců 12 lidí a toto číslo se každým rokem zvyšuje. Lze rozlišit následující faktory ovlivňující růst počtu kybernetických trestných činů:

[6] DJERF–PIERRE, Monika. Squaring the Circle: public service and commercial news on Swedish television 1956?99. Journalism Studies [online]. 2000, 1(2), 239–260 [cit. 2023–01–29]. ISSN 1461–670X. Dostupné z: doi:10.1080/14616700050028235

- globální informatizace všech sfér života společnosti se nezvyšuje, ale snižuje stupeň její bezpečnosti;
- urychlení vědeckého a technického pokroku zvyšuje pravděpodobnost, že zločinci budou využívat čistě mírové technologie jako prostředky ničení a možnost jejich „dvojího“ použití je často nejen nepředvídaná, ale ani si ji tvůrci technologie neuvědomují;
- terorismus se stále více stává zvláštním typem informační technologie, protože:

za prvé, teroristé stále více využívají schopnosti moderních informačních a telekomunikačních systémů pro komunikaci a shromažďování informací;

za druhé, realitou našich dnů je takzvaný „kybernetický terorismus“;

za třetí, většina teroristických činů je v současnosti zaměřena nejen na způsobení materiálních škod, ohrožení lidských životů a zdraví, ale také na vyvolání informačního a psychologického šoku, jehož dopad na velké masy lidí vytváří příznivou situaci, v níž teroristé mohou dosáhnout svých cílů;

- „digitální propast“ a vznik zemí, které prohrály informační závod nebo prohrávají, se může stát příčinou teroristických aktivit proti jednotlivým státům jako prostředku asymetrické reakce.[7]

Hlavními objekty kybernetických hrozeb jsou:

občané: Ovlivňování člověka shromažďováním osobních dat a útoky na osobní počítače a mobilní zařízení občanů, úniky a zveřejňování soukromých informací, podvody, šíření nebezpečného obsahu.

podnikatelské struktury: Dopad na systémy internetového bankovnictví, dopad na informační infrastrukturu, blokování online obchodních systémů, geoinformační systémy a útoky hackerů na firemní weby.

[7] WikiSofia: Digitální propast. Definice digitální propasti, základní dimenze digitální propasti, demografické skupiny nejvíce ohrožené digitální propastí ve vyspělém světě [online]. Univerzita Karlova v Praze, Filozofická fakulta, 2013-2017 [cit. 2023-02-07]. Dostupné z: https://wikisofia.cz/

stát: Útoky na klíčovou infrastrukturu státu (eGovernment, webové stránky státních institucí), ekonomický úsek (rozsáhlé odpojování platebních systémů, rezervační systémy), hardwarové útoky na osobní počítače a kritickou infrastrukturu státních podniků.

S tím, jak je přístup k internetu spolehlivější a počet lidí připojených k internetu se zvyšuje, roste i počet důležitých služeb poskytovaných online. 63 % světové populace se může připojit k internetu. V uplynulém roce mělo přístup k internetu 200 milionů lidí. Ne každý má však stejnou úroveň kvality tohoto spojení. V jižní Asii je většina lidí „mimo internet“. Více než polovina obyvatel Indie – 53 % neboli 744 milionů – nemá přístup k síti. Lidé tráví na internetu v průměru 6 hodin a 53 minut denně, což je o čtyři minuty méně než na začátku roku. To znamená, že uživatelé tráví v průměru asi 40 % svého času online, když jsou vzhůru.

Mladí lidé tráví na internetu více času než ostatní kategorie. Zároveň jsou absolutními lídry v ukazatelích ženy ve věku 16 až 24 let. Tři hlavní důvody pro návštěvu internetu zůstávají stejné: vyhledávání informací (60,2 %), udržování kontaktu s přáteli a rodinou (54,7 %) a vyhledávání novinek a událostí (52,3 %). Obecně platí, že každý čtvrtý člověk na světě vlastní nějakou kryptoměnu.

Mezi pět nejoblíbenějších webových stránek mezi uživateli na celém světě patří YouTube, Google, Facebook, Wikipedia a Pornhub.[8]

Je třeba poznamenat, že ne všechny případy porušování legislativy v oblasti informačních technologií nebo s použitím technických zařízení nové generace směřují k obohacení. S určitou mírou pravděpodobnosti lze tedy předpokládat, že mnoho zločinců v informační sféře využívá své výjimečné schopnosti k výdělku, ale nejčastěji je hacking a vyzrazení důvěrných dat spojeno se snahou informačních aktivistů ovlivnit veřejné mínění, změnit průběh politických procesů, předat zprávu masám nebo šířit určitou myšlenku.

[8] DIGITAL 2022: OCTOBER GLOBAL STATSHOT REPORT [online]. 20 OCTOBER 2022n. l. [cit. 2023-02-01]. Dostupné z: https://datareportal.com/reports/digital–2022–october–global–statshot

V rámci mého kriminologického šetření je třeba upozornit na nejvýznamnější představitele mezinárodních zločineckých skupin působících a existujících v rámci informačních systémů, kteří s největší pravděpodobností jednají z politického hlediska.

První hackerská skupina má název *Anonymous International* nebo jak ji bylo nazýváno pro snadné osvětlení komunitou „*Humpty Dumpty*", a to protože všechny zprávy a „splachy" informací zveřejněných na síti členy tohoto sdružení byly zveřejněny jménem fiktivní postavy. Anonymous – mezinárodní skupina, která má velký počet účastníků z celého světa.

Specialisté této skupiny zločinců působí již dlouhou dobu zhruba od roku 2003, a jejich cílem jsou vládní sítě, náboženské a firemní webové stránky a účty úředníků a veřejně činných osob. Tato skupina využívá všech metod kyberkriminality k prosazování politických myšlenek a šíření svobody slova, ochrany lidských práv, svobody pohybu informací. Motto této organizace je kombinací vět: „*Je nás mnoho, nezapomínáme, neodpouštíme, počkejte si na nás.*"[9] Nejednoznačnost chování této skupiny umožnila vytvoření množství fám a legend kolem jejich skutečných cílů, nicméně fakta naznačují, že cílem tohoto hnutí je vidět svobodu slova a informací, odhalování korporátních lží a nerovnosti, jakož i dosažení politické pravdy, což tato skupina dělá spíše „myšlenkou hnutí" po celém světě, zejména s ohledem na výzvy k účasti, které „hacktivisté" opouštějí po sérii útoků.

Také třeba poznamenat, že toto hnutí má stránky v různých sociálních sítích, kde jsou zveřejňována jejich vyjádření k jakýmkoliv událostem či osobnostem v různých obdobích. Tak, kupříkladu jedna z jejich stránek obsahuje názory na video na téma posledních voleb v USA, která zveřejňuje informace získané pravděpodobně nelegálně o zneuctění cti a důstojnosti prezidenta USA D. Trumpa.

[9] YAR, Majid. The Novelty of 'Cybercrime'. European Journal of Criminology [online]. 2005, 2(4), 407–427 [cit. 2023–01–29]. ISSN 1477–3708. Dostupné z: doi:10.1177/147737080556056
Kessel J. M. and Mozur P. How China Is Changing Your Internet [online]. New York Times: 2017

Další skupinou, která provedla politické útoky byla hackerská skupina s názvem *LulzSec* nebo *TheLulz Boat*, jejímž původním heslem bylo: „*smát se vaší (kyber) obraně od roku 2011”*. Navzdory své relativně krátké historii (účastníci byli zadrženi v červnu 2011) byla skupina vytvořená původně „pro smích“ známá řadou významných zločinů proti informačním sítím nejen společností, které byly v té době považovány za chráněné, ale také oficiální stránky Senátu Spojených států amerických, stránky Ústřední zpravodajské služby USA, stránky společnosti Sony (11 milionů účtů) a sociální síť pro vojenský personál (na které hackli 170 tisíc osobních stránek), jakož i různé kompromitující údaje o představitelích americké vojenské elity.[10]

Členové hackerské skupiny zveřejnili na síti všechny otevřené důvěrné informace a také otevřeně podpořili zakladatele WikiLeaks D. Assange. V jednom z rozhovorů účastník projektu LulzSec, hacker s krycím jménem Vir, který si říkal „kapitán lodi Lulzim“, upřesnil, že skupinu zpočátku tvořilo 6 specialistů, kteří nejprve hráli pro smích, ale pak přešel na „politicky motivované útoky“.

Další skupinou hackerů, kteří páchají zločiny na základě svých politických názorů je Syrská elektronická armáda (*Syrian Electronic Army*). Vznik této skupiny je spojen se začátkem občanské války v Sýrii v roce 2011. Podle odborníků je skupina specialistů, která podporuje prezidenta Bašára al–Asada, zapojena do mnoha významných politických případů v informačním prostoru, včetně háckování webových stránek zpravodajských agentur New York Times a Huffington Post a dalších významných médií v roce 2014 účty bývalého prezidenta USA B. Obamy a bývalého prezidenta Francie – Nicolase Sarkozyho.[11]

Hackerská a špionážní skupina Fancy Bear používá stejné metody a prostředky k páchání trestných činů v kyberprostoru, jejichž cílem jsou státní

[10] Kessel J. M. and Mozur P. How China Is Changing Your Internet [online]. New York Times: 2017 Digital Storytelling Contest, Short Form, 3rd prize, vysíláno dne 2017 [cit 2023-01-22]. Dostupné z: –wechat.html.

[11] SANDERS Karen, Canel Crespo María José, and Holtz–Bacha Christina. Communicating Governments: A Three–Country Comparison of How Governments Communicate with Citizens. The International Journal of Press/Politics, [online]. 16(4). 2017. 547 p. [cit. .2023-01-22]. ISSN v DOI:10.1177/1940161211418225. Dostupné z: https://mariajosecanel.com/

představitelé různých zemí včetně USA a Německa, stejně jako Mezinárodní olympijský výbor a světová antidopingová agentura – WADA.

Tato skupina je také obviněna z hackování německých vládních informačních systémů, získání přístupu na servery strany CDU a osobní korespondence německé kancléřky Angely Merkelové. Němečtí specialisté resortních služeb odmítli potvrdit spojitost těchto útoků s ruskými hackery, nicméně bylo zjištěno, že tito hackeři jsou již známy svými útoky na vnitřní sítě Bundestagu a jsou pravděpodobně napojení na Hlavní zpravodajské ředitelství ozbrojených sil Ruské federace.

Seznam uvedený v této bakalářské práci jen částečně odráží obecný trend rostoucích případů pronikání, nelegálního přístupu, hackování a využívání informačních sítí vlád, státních zastoupení, organizace, nadace atd. s cílem změnit politickou situaci, zprostředkovat určitý postoj, ovlivňovat politické procesy.

V této části bych se také ráda zmínila o aktuálním stavu kyberkriminality v České republice. Z dlouhodobého hlediska má kyberkriminalita v České republice poměrně stabilní a vysoký růst. Potvrdil se očekávaný trend, tedy postupný přesun kriminálních aktivit do kyberprostoru. Trestné činy spáchané v kyberprostoru (18 554 činů) mezi lednem a prosincem 2022 tvořily 10,2 % z celkového počtu registrovaných trestných činů. Trend je podle statistik neustále stoupající (meziročně více než 94,9 %).

Dlouhodobě je evidován poměrně stálý růst nápadu této registrované trestné činnosti, kdy k poslednímu dni v prosinci 2022 stoupl meziročně počet skutků, tzv. „hackingu“ o více jak 53 %. Konkrétně bylo do konce prosince 2021 evidováno 1682 těchto skutků, přičemž do konce letošního prosince bylo evidováno již 2575 těchto skutků.[12]

Ze stávajících dat lze předvídat rostoucí trend kybernetických útoků a do konce roku 2023 můžeme předpokládat, že počet registrovaných trestných činů kyberkriminality přesáhne 30 000.

[12] Policie ČR: Vývoj registrované kriminality v roce 2022 [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

1.3. Kyberkriminologie

Neustálá aktualizace kriminologických poznatků, podmíněná jak vnitřními zákonitostmi vývoje vědy o kriminalitě, tak i změnami probíhajícími ve společnosti, kumulovaným objemem kriminologických poznatků si vyžádala vyčlenění „rozšířených" kriminologických celků ve struktuře kriminologie, které bývají označovány jako soukromé kriminologické teorie. Z nich má v současné fázi vývoje největší význam kyberkriminologie, odvětví kriminologických poznatků, které zkoumá trestnou činnost spojenou s využíváním počítačových a informačních technologií i globálních sítí.

Cílem této části je odhalit pojem a předmět kyberkriminologie jako jedné z nejaktuálnějších oblastí kriminologického vědeckého poznání a analyzovat kyberkriminalitu prizmatem kriminologie.

Rozvoj informačních technologií v posledních desetiletích vede k nové, tzv. digitální realitě, digitální transformaci sociálních vztahů. Digitální technologie pronikají do zavedených vztahů a institucí a digitalizace se stává ústředním prvkem transformace ekonomiky, sociální sféry a politické a právní regulace.

S rostoucím počtem kritických služeb nabízených online se rozšiřují možnosti zneužití technologií a páchání trestné činnosti. Zvláštní výzvou je zajištění minimalizace kriminogenních rizik ve vyvíjející se digitální realitě, včetně vývoje opatření proti kyberkriminalitě a viktimologické prevence pro oběti trestných činů v informačně-digitální oblasti.

Mezi nejoblíbenější typy kyberzločinců patří používání malwaru, phishing a krádeže pomocí výpočetní techniky. Tyto trestné činy představují až třetinu všech trestných činů v oblasti kybernetické kriminality. Vědecké zkoumání kyberkriminality začalo téměř ihned poté, co se s rozvojem digitálních technologií rozšířila po celém světě.

Termín „kyberkriminologie" je však nový a není všeobecně uznávaný. Tvrdí se, že tento termín vymyslel renomovaný indický výzkumník K. Jaishankar, který

od roku 2007 vydává online časopis International Journal of Cyber Criminology[13] a publikoval řadu článků o této problematice.[14] Je třeba také poznamenat, že neexistuje všeobecně přijímaná definice kyberkriminality jako základního předmětu studia kyberkriminologie. Je také důležité zdůraznit, že česká kriminologie takový pojem nezná a v podstatě neuznává.

V doktríně a právních pramenech se používá také pojem „kyberkriminalita" spolu s pojmy jako „počítačová kriminalita", „internetová kriminalita", „high–tech kriminalita"[15] a často se tyto pojmy zaměňují.

Zvláštností kyberkriminality je, že se jedná o nadnárodní trestnou činnost, jejíž pachatelé a oběti se mohou nacházet kdekoli na světě, kde jsou připojení k internetu. Vyšetřovatelé kyberkriminality proto často potřebují přeshraniční přístup k údajům a jejich sdílení. Mezi hlavní právní problémy při vyšetřování a stíhání kyberkriminality patří:

- rozdílné právní systémy jednotlivých států;
- rozdíly ve vnitrostátních právních předpisech týkajících se kyberkriminality;
- rozdíly v důkazních pravidlech a trestních řízeních (například postupy pro orgány činné v trestním řízení při přístupu k digitálním důkazům);
- rozdíly v oblasti působnosti a zeměpisné použitelnosti regionálních a mnohostranných smluv o kyberkriminalitě;
- rozdíly v přístupu k ochraně údajů a lidských práv atd.

Kyberkriminalita se stává stále závažnějším problémem pro země s dobře rozvinutou internetovou infrastrukturou a fungujícími platebními systémy. Nedávná hodnocení Interpolu týkající se hrozby kybernetické kriminality ukazují,

[13] International Journal of Cyber Criminology [online]. 2020 [cit. 2023-02-13]. ISSN 0974–2891. Dostupné z: http:// www.cybercrimejournal.com.

[14] K., Jaishankar. Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology [online]. 2018. – January–June. – Vol. 12 [cit. 2023-02-13]. Dostupné z: https:// pdfs.semanticscholar.org/4146/e6a16b448d63d476fce0a3a81554b1852438 pdf.

[15] High Technology Crime Law and Legal Definition. Uslegal [online]. [cit. 2023-02-28]. Dostupné z: https://definitions.uslegal.com/h/high-technology-crime/

že se stává stále agresivnější a konfrontačnější. To se projevuje v různých formách kyberkriminality, včetně trestné činnosti v oblasti špičkových technologií, úniku dat a sexuálního vydírání.

Analýza hlavních faktorů, jakož i příčin a podmínek, které ovlivnily stav kriminální situace v oblasti informační bezpečnosti v České republice, dává důvod se domnívat, že v následujících letech bude formování kriminologických parametrů jak v republice jako celku, tak v jejích regionech probíhat v podmínkách zvláštností, které byly pozorovány v předchozím období.

Předpokládá se, že dynamický rozvoj IT průmyslu v zemi, provozování hazardních her atd. objektivně a nevyhnutelně přispěje k nárůstu kyberkriminality. Vezmeme-li přitom v úvahu globální trendy, měli bychom v prvé řadě očekávat další nárůst krádeží prostřednictvím využívání výpočetní techniky a případů neoprávněného přístupu k informacím z počítače, spáchaných zejména podvodnými metodami, např. phishing a hackování uživatelských účtů na sociálních sítích.

Specifická váha kyberkriminality je vzhledem k její vysoké latenci ve skutečnosti výrazně vyšší. Podle průzkumů mezi obyvateli se s kyberkriminalitou setkal každý čtvrtý. Odborníci odhadují, že pouze ti, kteří nepoužívají internet a nevlastní chytrý telefon, se mohou považovat za chráněné před kyberkriminalitou.

Tyto údaje naznačují, že tento typ kriminality se v budoucnu stane jednou z významných hrozeb pro kriminologickou bezpečnost. Rozvoj výzkumu v rámci kyberkriminologie zahrnuje nejen tradiční kriminologickou analýzu kvantitativních a kvalitativních ukazatelů kyberkriminality, jejích determinant, identity kyberzločinců, opatření k prevenci kyberkriminality, ale studuje i využití informačních technologií jako nástroje k potírání hrozeb pro osobní, státní a veřejnou oblast (např. využití digitálního profilování (rastrové vyhledávání trestných činů v pátrací praxi)).

V zájmu zlepšení kvality a účinnosti tohoto poznání je třeba zřídit středisko pro studium kyberkriminality, které by bylo centrem odborných znalostí v oblasti

trestního práva a řízení, informačních technologií, kriminologie, kriminalistiky a vzdělávání v této oblasti.

2. Kriminologická analýza kyberzločinců a zločinu v kyberprostoru

2.1. Kyberkriminalita a její druhy

Je třeba poznamenat, že v současné době nemá ani vnitrostátní legislativa, ani teorie trestního práva jednotný ustálený postoj ke klasifikaci kyberkriminality. Navíc neexistuje shoda na tom, které konkrétní trestné činy by měly být klasifikovány jako trestné činy proti kybernetické bezpečnosti. V zásadě lze kyberprostor v dnešní době využít k tomu, aby prostřednictvím kyberprostoru bylo možno spáchat celou řadu trestných činů: od úmyslné vraždy (například vyřazením umělého dýchacího systému pacienta nebo zastavením „umělého srdce“ nebo zásahem do počítačového systému jedoucích vozidel) až po krádež peněz nebo podvod s jiným majetkem; od kybernetické špionáže a kyberterorismu po prodej předmětů zakázaných pro volný oběh (střelné zbraně, omamné a psychotropní látky, pornografické předměty atd.); od neoprávněného zasahování do provozu elektronických počítačů, automatizovaných systémů, počítačových sítí nebo telekomunikačních sítí po válečnou propagandu atd.

V právní literatuře se počítačové trestné činy (přestupky) klasifikují na tři skupiny:

1) trestné činy, jejichž předmětem je samotný počítač nebo informace v něm obsažené protiprávních činů;

2) trestné činy, při nichž je počítač použít jako nástroj trestného činu;

3) trestné činy, jejichž důkazem jsou informace obsažené v počítačových systémech.

Rozšíření internetu a zařízení, která jsou k němu připojena, je nepochybně důležité, zejména v jednadvacátém století, kdy poskytují možnosti a výhody pro vzdělávání, podnikání a online sítě a komunikaci, které v období celosvětové

pandemie COVID–19 v letech 2020–2021 nabývají na významu. Přestože je tato technologie pravděpodobně silou dobra, nabízí také nebývalé možnosti škod. Ti, kteří chtějí škodit, se pohybují ve stejném online prostoru a hledají příležitosti.[16]

Zneužití této technologie otevřelo kyberzločincům nové možnosti, jak škodit jednotlivcům, podnikům a podnikání. Vzhledem ke vlivu technologií na náš každodenní život a na kriminalitu, budeme níže věnovat pozornost nejčastějším kybernetickým trestným činům:

Phishing

Je jedním z nejčastějších způsobů krádeže osobních údajů uživatelů. Při phishingu se kyberzločinci obvykle vydávají za legitimní zástupce organizace, aby od obětí získali citlivé údaje, například hesla a čísla kreditních karet.[17]

Phishingové e-maily

Mají obvykle vypadat jako oficiální e-maily od různých finančních institucí, daňových úřadů nebo jiných organizací a mají lidi přimět k poskytnutí osobních údajů. Tyto podvodné praktiky obvykle zahrnují zasílání e-mailů nebo telefonátů, v nichž jsou příjemci informováni, že musí okamžitě aktualizovat údaje o svém účtu, jinak jim hrozí zablokování. Tento typ podvodu se v posledních letech stal velmi populárním, protože pachatele je obtížné vypátrat a jejich realizace není složitá. Společnost Wandera, která se zabývá bezpečností IT, tvrdí, že každých 20 sekund vznikne nová phishingová stránka.[18]

Tímto způsobem každou minutu tak vznikají tři nové phishingové webové stránky, které vystavují podniky potenciálním hrozbám. Nejlepším způsobem, jak se vyhnout tomu, abyste se nestali obětí, je poučit zaměstnance o příznacích podvodných e-mailů a vypracovat bezpečnostní zásady, jak mají zaměstnanci postupovat, pokud mají podezření, že e-mail může být falešný.

---

[16] YOUNG, Suzanne a Katie STRUDWICK. Teaching Criminology and Criminal Justice: Challenges for Higher Education. Palgrave Macmillan, 2022. ISBN 978–3–031–14898–9.
[17] Kaspersky: What is Pharming and how to protect yourself [online]. [cit. 2022-07-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming
[18] Mobile Threat Landscape 2020: Understanding the key trends in mobile enterprise security in 2020 [online]. 2020, 13 [cit. 2023-01-31]. Dostupné z: http://go.wandera.com/rs/988–EGM–040/images/Mobile%20Threat%20Landscape%202020.pdf

Hacking

Neoprávněný přístup k počítačovému systému a nosiči informací s cílem infikovat počítač oběti nebo obejít bezpečnostní opatření. Hackeři jsou ti, kteří využívají své znalosti k identifikaci zranitelných míst v počítačovém systému. V důsledku toho mohou společnosti čelit různým problémům (od nabourání se do počítačového systému až po získání přístupu k důvěrným údajům).[19] Hackeři mohou dokonce zničit pověst společnosti tím, že o ní zveřejní důvěrné informace. Někdy se jim také říká hacktivisté („hacktivists“).[20]

Existují tři typy hackerů:

„*etický hacker*“ využívající své schopnosti k nalezení chyb v softwaru dříve než útočníci – hlásí chyby, aby mohly být rychleji opraveny.[21]

***„černý klobouk*“** vytváří programy určené k nabourání se do počítačů jiných uživatelů, umožňuje krást informace a prodávat je na Dark Webu.

„šedý *klobouk*“ používá metody, které se pohybují mezi těmito dvěma extrémy – snaží se identifikovat zranitelná místa v systému a postupy, které mohou porušovat zákony nebo etické normy.[22]

Nelegální těžba kryptoměn (cryptojacking, skrytý cryptomining)

Je druhem kybernetické kriminality, při níž hackeři nelegálně využívají cizí počítače a sítě k získání kryptoměn. Podle společnosti SonicWall se v první polovině roku 2022 zvýšil celosvětový objem kryptografických útoků na 66,7

[19] KYBERKRIMINALITA: Jednotlivé druhy kyberkriminality. Policie České republiky [online]. [cit. 2023-01-31]. Dostupné z: https://www.policie.cz/clanek/jednotlive–druhy–kyberkriminality.aspx
[20] ANDRESS, Jason a Steve WINTERFELD. Cyber Warfare.: Hacktivist [online]. 2016, 207–219 [cit. 2023–01–31]. Dostupné z: https://www.sciencedirect.com/topics/computer–science/hacktivist
[21] MUELLER, Annie. Famous White–Hat Hackers [online]. In:. Uptáte July 16, 2022 [cit. 2023-02-01]. Dostupné z: https://www.investopedia.com/financial–edge/0811/famous–white–hat–hackers.aspx
[22] Black had, White hat, and Gray hat hackers – Definition and Explanation. Kaspersky [online]. 2023 [cit. 2023-02-01]. Dostupné z: https://www.kaspersky.com/resource–center/definitions/hacker–hat–types

milionu, což je o 30 % více než v první polovině roku 2021. Největší dopad měl 269% růst na finanční odvětví.[23]

Jedním z hlavních problémů cryptojackingu je nadměrné zatížení procesoru, které vede k výraznému zpomalení provozu systémů nebo dokonce k jejich úplnému selhání. Někdy se tak stane dříve, než si společnosti uvědomí, že došlo ke spáchání kybernetického trestného činu. Organizace se mohou před tímto typem zločinu chránit tím, že odborník na informační systémy pravidelně kontroluje systém, zda nedochází k neobvyklým nárůstům zatížení procesoru.

Spoofing

Druh kybernetické trestné činnosti, kdy někdo změní svou online identitu, aby oklamal jiného uživatele. Mezi tyto trestné činy může patřit změna e-mailových adres, telefonních čísel, profilů na sociálních sítích a inzerátů. Ukázkovým příkladem je situace, kdy hacker odešle e-mail vydávající se za e-mail kolegy z práce a požaduje důvěrné firemní informace. Kyberzločinci mohou také vytvářet webové stránky, které vypadají jako oficiální stránky různých společností, ale jsou určeny ke shromažďování osobních údajů. Nejlepší způsob, jak se těmto podvodným praktikám vyhnout, je zkontrolovat odkazy před kliknutím na ně nebo zadáním jakýchkoliv informací. Měli byste se mít na pozoru před nevyžádanými emaily, které požadují hesla, čísla finančních účtů nebo jiné citlivé informace o uživateli.[24, 25]

Ransomware

Ransomware je typ malwaru, který napadá počítačové systémy, blokuje data a požaduje platbu za jejich odblokování. Jakmile je počítač infikován

[23] 2022 SonicWall Cyber Threat Report. SonicWall [online]. [cit. 2023-02-01]. Dostupné z: https://www.sonicwall.com/2022–cyber–threat–report/

[24] What is Spoofing – Definition and Explanation [online]. [cit. 2023-02-28]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/spoofing

[25] Policie ČR: PREVENTIVNÍ INFORMACE. Vishing a spoofing [online]. [cit. 2023-03-01]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

ransomwarem, je uživatel požádán o zaplacení výkupného, aby získal dešifrovací klíč potřebný k získání kontroly nad daty.[26, 27]

Průměrné náklady na útok ransomwarem jsou více než 4 miliony dolarů, zatímco na destruktivní útok v průměru více než 5 milionů dolarů. Nákaze ransomwarem lze často zabránit dodržováním základních bezpečnostních postupů, jako je aktualizace operačního systému nebo neklikání na podezřelé odkazy či přílohy od neznámých odesílatelů.

Cross–site scripting (XSS)

Je zranitelnost zabezpečení webu, ke které dochází, když útočník vloží do důvěryhodného webu nebo webové aplikace škodlivé skripty. XSS umožňuje útočníkům získat kontrolu nad relací uživatele, ukrást jeho přihlašovací údaje a shromažďovat cenné firemní informace. Útočníci mohou například na napadené webové stránky umístit škodlivý kód a čekat, až se nic netušící uživatel přihlásí, aby z počítače oběti získali citlivé informace. Tyto zranitelnosti někdy umožňují útočníkům převzít relaci a zcela se vydávat za oběť.[28]

Existují tři typy XSS – uložený XSS, reflektovaný XSS a XSS založený na DOM (Document Object Model). Uložený XSS. Útočníci tento typ zneužití používají ke stažení malwaru nebo ke krádeži souborů cookie obsahujících citlivé osobní údaje, jako jsou hesla a čísla kreditních karet. Odražený XSS. Spustí se, když oběť klikne na odkaz na napadeném webu, který v prohlížeči aktivuje skript obsahující škodlivý kód. Prohlížeč oběti odešle skript zpět na útočící server. XSS založený na DOM. Zneužívá zranitelnosti v DOM nebo ve způsobu, jakým prohlížeče zpracovávají dokumenty HTML. Cílem tohoto útoku je přinutit prohlížeč provést změny, které vytvoří zranitelnosti, a to manipulací s objekty JavaScriptu, jako je XMLHttpRequest nebo WebSocket. Aby se společnosti ochránila před

[26] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 390-407 ISBN 978-80-7598-554-5.
[27] KOLOUCH, Jan a VOLEVECKÝ, Petr. Trestněprávní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. s. 40-41. ISBN 978-80-7251-402-1.
[28] KirstenS. Cross Site Scripting (XSS) [online]. [cit. 2023-02-01]. Dostupné z: https://owasp.org/www–community/attacks/xss/

všemi třemi typy cross–site scripting, musí zavést bezpečné techniky kódování, jako je propojování a zajistit správnou validaci vstupů.[29]

Krádež identity

Je druh počítačové kriminality, při níž osoba zneužívá cizí totožnost, například jméno a číslo pojištění, číslo bankovního účtu a údaje o kreditní kartě, ke spáchání podvodu. Špatní „herci“ mohou poškodit dobrou pověst oběti a zničit její úvěrovou historii. Hackeři shromažďují informace o uživatelích různými metodami, včetně nabourávání se do počítačů, krádeží e-mailů, zachycování dat z obrazovek počítačů a vytváření falešných kopií identit nic netušících obětí. Kyberzločinci pak tyto informace využívají k tomu, aby se vydávali za oběti, žádali o půjčky, ovládali jejich finance a získali přístup k jejich bankovním účtům. Abyste se vyhnuli krádeži identity, měli byste se o dokumenty obsahující citlivé informace řádně starat: před vyhozením je rozstříhejte na kousky a nepoužívejte veřejné odpadkové koše.[30]

Úvěrový podvod

Při úvěrovém podvodu se pachatel vydává za zástupce společnosti a požaduje platbu za zboží nebo služby, které nikdy nebyly poskytnuty. Tyto podvody jsou obvykle úspěšné, protože falešná faktura je zaslána účetnímu oddělení, které dodavatele osobně nezná. Podniky jsou vůči tomuto typu podvodu nejzranitelnější, když rozšiřují své aktivity a přechází z malé společnosti na střední nebo velkou firmu. Zločinec se může vydávat za zaměstnance, který jménem společnosti žádá o finanční prostředky nebo dokonce může jít tak daleko, že vytváří falešné faktury, které vypadají jako legitimní. Pokud jde o kybernetickou kriminalitu, společnosti musí mít systém kontrol a rovnováhy, který se opírá o více zaměstnanců v rámci organizace, například vyžadovat více podpisů pro všechny platby nad určitou částku.

[29] Cross–site scripting (XSS) [online]. [cit. 2023-02-22]. Dostupné z: https://www.enisa.europa.eu/
[30] SCHEINOST, PhDr. Miroslav a JUDr. Zdeněk KARABEC, CSC. Zneužití identity a trestná činnost s tím spojená. Institut pro kriminologii a sociální prevenci, Praha [online]. [cit. 2023-03-07]. Dostupné z: https://www.mvcr.cz/soubor/scheinostkarab-identity-pdf.aspx

Malware

Hackerský software určený k narušení provozu počítače, shromažďování důvěrných informací nebo získání vzdáleného přístupu. Malware často zůstává neodhalen, je obtížné jej odstranit a může způsobit značné škody na počítačových systémech tím, že infikuje soubory, mění data a ničí systémové nástroje. Je důležité si uvědomit, že malware se může maskovat jako běžný software, což usnadňuje jeho průnik do počítače oběti. Příkladem takových programů jsou viry, červi, trojské koně, spyware a adware.[31]

Sociální inženýrství

Umění manipulace s lidmi za účelem získání důvěrných informací nebo pověření. Tato praktika spočívá v tom, že se vydávají za zaměstnance společnosti, telefonují, posílají emaily a využívají služby rychlého zasílání zpráv, aby si získali důvěru oběti. Zločinec žádá o informace, jako jsou hesla a osobní identifikační čísla (PIN). Statistiky ukazují, že 98 % všech kybernetických zločinů zahrnuje nějakou formu sociálního inženýrství. Oběti jsou nejen podvedeny, aby prozradily své osobní údaje, ale mohou také nevědomky prozradit obchodní tajemství a sdílet duševní vlastnictví společnosti. Zavedení plánu reakce na takové incidenty bude velkou prevencí tohoto typu trestné činnosti.[32]

Podvádění s technickou podporou

Při těchto podvodech se podvodník vydává za zástupce známé společnosti a volá potenciálním obětem s tvrzením, že v jejich počítačích našel hrozby. Tyto hrozby mohou sahat od malwaru až po viry, které lze opravit za poplatek. Poté je podvodník přiměje ke vzdálenému přístupu do systému, což mu umožní požadovat ještě více peněz nebo ukrást osobní údaje. FBI uvádí, že manželé z Maine přišli o 1,1 milionu dolarů poté, co obdrželi vyskakovací okno s upozorněním, že jejich počítač byl napaden hackery a byl učiněn pokus o kompromitaci jejich bankovních údajů. Podvodníci se zaměřují na stresované lidi, kteří jsou zranitelní a ochotní zaplatit cokoli, aby se ochránili. Oběti si mohou

[31] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC.ISBN 978-80-88168-15-7.
[32] Národní úřad pro kybernetickou a informační bezpečnost – Sociální inženýrství 2016. [online]. [cit. 2023-03-06] Dostupné z: https://nukib.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/

uvědomit, že se staly obětí podvodu, až když je příliš pozdě, protože podvodník jim poskytl aktualizace softwaru, které je přesvědčili, že jsou v bezpečí. Podvodníci manžele přesvědčili, aby převedli peníze z jejich penzijního účtu, a poté s nimi přerušili veškerou komunikaci.

Nabourávání se do zařízení IoT

Jedna z nejčastějších forem počítačové kriminality. K tomuto útoku dochází, když hacker použije zařízení připojené k internetu, například chytrý termostat nebo ledničku. Naboural se do zařízení, infikuje ho malwarem a rozšíří ho do celé sítě. Hackeři používají infikované systémy k útokům na další systémy v síti. Tyto útoky mohou často vést ke krádeži dat ze zařízení a umožnit podvodníkům přístup k citlivým informacím. Riziko ohrožení zařízení internetu věcí vzniká proto, že tato zařízení mají omezené zabezpečení, výpočetní výkon, paměť a úložnou kapacitu. To znamená, že je u nich větší pravděpodobnost zranitelnosti než u jiných systémů.[33]

Počítačové pirátství

Nelegální kopírování, distribuce nebo používání softwaru bez vlastnického nebo zákonného povolení. K tomu může dojít stažením softwaru z nelegálních webových stránek, kopírováním softwaru z jednoho počítače do druhého nebo prodejem jeho kopií. Pirátský software ovlivňuje zisky společnosti, protože jí brání vydělávat na svých produktech. Software Alliance zjistila, že 37 % softwaru nainstalovaného v osobních počítačích je nelicencovaný nebo pirátský. Jelikož se jedná o celosvětový problém, je důležité, aby společnosti věděly, jak mohou být postiženy a jaké metody ochrany mají k dispozici.[34]

Trojský kůň

Virus, který se vydává za běžný program a instaluje se do počítače bez svolení uživatele. Po spuštění může provádět akce, jako je mazání souborů,

[33] Internet věcí používá v Česku třetina firem. Čidla mohou být ale terčem hackerských útoků. Tematický speciál E15 [online]. [cit. 2023-03-07]. Dostupné z: https://www.e15.cz/tematicke-specialy/kyberneticka-bezpecnost/internet-veci-pouziva-v-cesku-tretina-firem-cidla-mohou-byt-ale-tercem-hackerskych-utoku-1392728

[34] Software Management: Security Imperative, Business Opportunity: 2018 BSA GLOBAL SOFTWARE SURVEY [online]. [cit. 2023-02-01]. Dostupné z: https://gss.bsa.org/

instalace dalšího malwaru a krádež informací, například čísel kreditních karet. Klíčem k zabránění takové podvodné činnosti je stahovat software pouze z důvěryhodných stránek, například z webových stránek společnosti nebo od autorizovaných partnerů.

Odposlech

Je skryté odposlouchávání nebo nahrávání rozhovoru bez vědomí a/nebo souhlasu stran. Může probíhat po telefonu, pomocí skryté kamery nebo dokonce prostřednictvím vzdáleného přístupu do systému. Tento postup je nezákonný a vystavuje uživatele riziku podvodu a krádeže identity. Svou společnost může chránit tím, že omezí informace, které zaměstnanci sdílejí prostřednictvím emailu. Účinnou ochranou by bylo také šifrování konverzací a používání speciálního softwaru, který brání neoprávněným uživatelům ve vzdáleném přístupu k síťovým zdrojům.[35]

Útoky DDoS a DoS

DoS představuje kybernetický útok typu odepření služby, při kterém dojde k zahlcení cílového serveru vysláním obrovského množství požadavků. Cílový server pak není schopen takové množství dat zpracovat a dochází k jeho přetížení, nefunkčnosti a nedostupnosti služby u ostatních oprávněných uživatelů. Při tomto typu útoku však fakticky nedochází k průniku útočníka do cílového systému, resp. útočník nezískává možnost data získat či s daty. Rozšířenou variantou útoku je pak DDoS (Distributed Denial of Service).[36]

DDoS jsou zaměřeny na službu nebo systém, který je zahlcen větším počtem požadavků, než je schopen zvládnout. Nekonečný proud požadavků nutí servery k vypínání, což narušuje dostupnost informací pro uživatele, kteří se k nim snaží získat přístup. Hackeři používají DDoS jako formu protestu proti webovým stránkám a jejich vedení, v některých případech však tyto útoky slouží také k

[35] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC.ISBN 978-80-88168-15-7.
[36] ŠŤASTNÝ, Mgr. Bc. Jakub. Trestní postih DoS/DDoS útoků. EPRAVO.CZ – Sbírka zákonů, judikatura, právo [online]. 20. 4. 2020 [cit. 2023-03-07]. Dostupné z: https://www.epravo.cz/top/clanky/trestni-postih-dosddos-utoku-110941.html

vydírání. Útoky DDoS mohou být výsledkem kybernetické špionáže, jejímž cílem je ukrást data organizace, nikoli je zničit.[37]

Pokročilá trvalá hrozba (Advanced Persistent Threat)

Typ kybernetického útoku, který je cílený, trvalý, sofistikovaný a má velké zdroje. APT se obvykle používají ke krádeži informací z organizace za účelem finančního zisku. Kybernetické útoky typu APT mohou trvat měsíce nebo dokonce roky. Proniknou do sítě, získají data a pak je bez odhalení odfiltrují. Typickými cíli jsou vládní instituce, univerzity, výrobní zařízení, high–tech průmysl a obranný sektor.[38]

Black Hat SEO

Optimalizace webových stránek pomocí technik zakázaných vyhledávači. Může se jednat o nacpání klíčových slov, neviditelný text a maskování, které způsobí, že si algoritmus vyhledávače myslí, že stránka je relevantní, i když tomu tak není. Takové marketingové techniky jsou nezákonné, protože porušují základy vyhledávání Google zneužitím systému řazení. V důsledku toho mohou optimalizátoři Black Hat dostat pokutu nebo mohou být jejich webové stránky zcela odstraněny ze stránky s výsledky vyhledávání.[39]

2.2. Determinaty kyberkriminality

Problematika příčin kriminality v kriminologii je klíčová, neboť určuje vědecký obsah kriminologické teorie a její praktické zaměření. Identifikace a zkoumání příčin a podmínek určitých druhů trestných činů a kriminality obecně umožňuje odhalit podstatu tohoto jevu, vysvětlit zákonitosti jeho vzniku,

[37] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 393-404. ISBN 978-80-7598-554-5.
[38] GHAFIR, Ibrahim a Václav PŘENOSIL. Advanced Persistent Threat and Spear Phishing Emails. In Miroslav Hrubý. Proceedings of International Conference Distance Learning, Simulation and Communication. první vydání. Brno, Czech Republic: University of Defence, 2015. s. 34-41. ISBN 978-80-7231-992-3.
[39] Kolda Ondřej. 7 black hat SEO technik, kterým se raději obloukem vyhněte [online]. 23. 07. 20210 [cit. 2023-03-07]. Dostupné z: https://www.blueghost.cz/clanek/7-black-hat-seo-technik-kterym-se-radeji-obloukem-vyhnete/

identifikovat trendy ve struktuře a úrovni kriminality, respektive určit strategii a vyvinout účinná preventivní opatření.

Samotné zkoumání role kyberprostoru jako média pro formování osobnosti pachatele a také souhrnu okolností, které existují nezávisle na osobě, osoby, která se dopustila trestného činu (prostředí trestného činu, které určuje okolnosti jeho spáchání) ve spojení s relevantními skutečnostmi reálného prostoru (sociálního prostředí) je základem pro pochopení zvláštností odhalování kyberkriminality a následně i pro úspěšný boj proti ní.

Zohlednění počtu pozdních typů deterministické interakce (z lat. determinare – způsobit existenci vývoj dalšího jevu pro označení všech jevů a procesů které hrají jakoukoliv roli v determinaci zločinu je vhodné používat termín – (fakta, determinanty).[40]

Za předpokladu určité podmíněnosti rozdělení určitých faktů determinace do určitých skupin se vzhledem ke složitosti interakce a složitosti dopadu na prototypické chování dále pokusím se definovat a analyzovat hlavní fakta determinaci kyberzločinu.

Politické a právní skutečnosti

Z pohledu politických procesů a politických faktorů se jedná o vznik kyberkriminality a rostoucí odpor vůči přítomnosti administrativně-teritoriálních a jiných hranic v globálních informačních sítích, nejednotnost postojů vlád různých zemí k otázkám svobodného šíření informací a ochrany práv a zájmů jednotlivců. Proces dosahování politické dohody o otázkách kyberkriminality komplikuje také rozdílné vnímání států v oblasti kyberkriminality které činy představují kyberkriminalitu a vyžadují kriminalizaci včetně vnímání morálního a etického rozměru těchto činů.

Předpokladem rozvoje informační společnosti je zajištění odpovídající úrovně kybernetické bezpečnosti. Kybernetická bezpečnost země je zajišťována

[40] CREWS, Gordon A. Wiley Online Library: Determinism. Wiley Online Library [online]. 26 March 2014 [cit. 2023-02-05]. Dostupné z: https://onlinelibrary.wiley.com/

prováděním státní politiky v souladu s doktrínami, zásadami, politikami a programy přijatými stanoveným postupem.

Ekonomické faktory.

Dnešní světová společnost vstoupila do informační fáze vývoje. V této fázi informační procesy stále více pronikají do všech oblastí lidské činnosti a stávají se účinným prvkem hospodářské politiky. Ekonomické skutečnosti týkající se určování kyberkriminality souvisejí především s procesem globalizace světové ekonomiky a globalizace obecně.

V současné době získává globální měřítko v souvislosti s globální ekonomikou modernizace společnosti prostřednictvím zavádění výpočetní techniky a technologických produktů, což přináší řadů inovací ve společenském životě. Jsou normy, které ztělesňují kybervirtualitu, kterou chápeme jako elektronicky a technicky založený typ virtuality, která je výsledkem technické tvořivosti sociálních aktérů využívajících počítačové vybavení a technologie a informační a komunikační technologií. Mobilní zařízení, osobní počítače a kybervirtualita se staly nejen neodmyslitelnými atributy a symboly modernosti, ale také faktory změn.[41] S uvedenými procesy souvisí určitá skupina ekonomických faktorů určování kyberkriminality. Tato skupina faktorů určujících kyberkriminalitu je podmíněna ekonomickým rozvojem a zaváděním špičkových technologií do životního stylu zemí „zlaté miliardy“.

Přístup ke globálním informačním sítím pro stále větší počet spotřebitelů, rozvoj elektronického obchodování, možnost otevření bankovních účtů přes internet a vznik možnosti dalších transakcí, které nevyžadují přímou smlouvu s protistranou, vedly k nárůstu příležitostí v oblasti online obchodování a transakcí s kreditními kartami, osobních údajů, průzkumů veřejného mínění a přístupu. Využívání špičkových technologií v podnicích vede k nárůstu průmyslové špionáže. Ekonomická stabilita a stabilní finanční situace kritiků ve vyspělých zemích je zároveň faktorem snadného přístupu k vlastní informační bezpečnosti.

[41] The Economic Impacts Of Cyber Crime: How It Costs Us All. Cyber security [online]. 30 June 2022 [cit. 2023-02-05]. Dostupné z: https://mitigatecyber.com/the–economic–impacts–of–cyber–crime–how–it–costs–us–all/

Je třeba poznamenat, že proces globalizace má i svou negativní stránku, která přímo souvisí s vymezením kyberkriminality. Odvrácenou stranou této skutečnosti je, že když jedni zbohatnou, druzí vždy zchudnou. A to je, jak známo, silný faktor, zejména v případě středních vrstev.

Rostoucí rozdíl mezi životní úrovní rozvojových zemí a zemí „zlaté miliardy“, finanční krize, které způsobují negativní procesy, a další související negativní jevy jsou rovněž faktory demytizace kyberkriminality.

Vzhledem k těmto faktorům je nárůst kyberkriminality jedním z důsledků všeobecné kriminalizace hospodářské činnosti v rozvíjejících se ekonomikách. To je případ Latinské Ameriky, bývalých zemí SSSR. Mnoho lidí a vlád hledá nové způsoby, jak vydělat peníze nebo jednoduše ušetřit, včetně těch kriminálních. Rostoucí nezaměstnanost a nedostatek vědeckých a technických talentů způsobují odliv intelektuálů z legální ekonomiky do kriminální.

Intenzivní informovanost a globalizace světa při absenci účinných mechanismů globální ekonomiky, politická a právní regulace (jak na úrovni jednotlivých států, tak na mezinárodní úrovni) těchto procesů vede ke kriminalizaci významné části komplexu. Zároveň platí, že čím nižší je úroveň ekonomického rozvoje země, politické a právní zajištění informační bezpečnosti, tím vyšší je úroveň kyberkriminality a kybernetických hrozeb obecně.

Organizační a administrativní faktory

Tato skupina faktorů souvisí především s nedostatky sociální kontroly. Ty se projevují zanedbáváním požadavků na bezpečnost informací ze strany vedoucích pracovníků podniků a soukromých subjektů a nedostatky ve finančním sektoru. Oběti kyberkriminality navíc z různých důvodů tyto zásady neoznamují orgánům činným v trestním řízení, To usnadňuje páchání trestných činů a zvyšuje riziko jejich páchání, což v důsledku vede ke zvýšení počtu spáchaných trestných činů. Mezi další nedostatky sociální kontroly patří nízká připravenost donucovacích orgánů na boj proti kyberkriminalitě a nedostatek kvalifikovaného personálu, nedostatečné technické znalosti, které spolu s obtížemi při řešení

kyberkriminality značně komplikují proces shromažďování důkazů a zadržení pachatele.

S rozvojem globálního počítačových sítí se rozšířila praxe cílené špionáže. Proto je dnes obzvláště důležitá problematika vývoje systémů ochrany a zachování státního, služebního a obchodního tajemství. V souvislosti s krádežemi služeb poskytovaných poskytovateli internetu vzniká řada problémů, včetně vniknutí do telefonních sítí a nelegálního obchodu s komunikačními službami. Internet je také hojně využíván obchodníky se softwarem, hardwarem, zbraněmi a drogami k obchodování, výměně informací, koordinaci činností a k získávání informací o drogách. Mezi organizačními a manažerskými faktory kyberkriminality hraje významnou roli organizace volnočasových aktivit v zemi, zejména pro mladé lidi.

Je třeba poznamenat, že různé druhy organizačních a administrativních opatření ze strany státu vedou nejen k tomu, že se stát snaží páchání kyberkriminality přecházet, ale také někdy vzniku kyberkriminality napomáhají.

Ideologická fakta

Úroveň kriminality v dané komunitě přímo závisí na úrovni její kultury. Výskyt kyberkriminality, stejně jako jiných druhů trestné činnosti, je spojen s negativními důsledky poklesu celkové úrovně kultury a morálních kritérií v naší společnosti.

Kyberkultura, jakožto samostatná sociální entita je institucionalizovanou a sebe reprodukující se hodnotou a ideologií. V procesu socializace a integrace soutěží s institucemi společnosti účastníci se musí socializovat současně dvěma způsoby: sociální totalitou kyberprostoru v zahraniční společnosti, kde interagují podle jejích vlastních charakteristik a v sociální komunitě kyberprostoru v širší společnosti, kde budou hrát podle jejích vlastních pravidel hry. Kromě zvládnutí norem a hodnot kyberkultury musí se internetový uživatel přizpůsobit své chování vlivu sociálních změn v reálné i virtuální společnosti. Dá se předpokládat, že v kyberkultuře má vzhledem k její vlivnější struktuře nárůst prvků individualizace

vyšší tempo než v kultuře dominantní. Je také zřejmé, že proces socializace v kyberprostoru neustále pokračuje.[42]

Podle odborníků ovlivňuje kyberprostor také motivace k trestné činnosti z následujících důvodů:

1) tento typ je extra typický a je založen na jiných konsolidačních faktorech;

2) v kyberprostoru dochází nejen k interakci, vzájemnému vzniku a mísení národních kultů, ale také k formování celého kulturního prostředí – kyberkultur.

Zároveň se v kyberprostoru, stejně jako ve skutečnosti v reálném světě sociálního systému, vyskytují stejné procesy v jejich kulturní fázi i se společenskými normami. Vzhledem k tomu, že kyberprostor hraje v životě mladých lidí významnou roli, dochází v myslích mladých aktivních uživatelů internetu k nahrazování sociálních norem normami kyberprostoru, lze tak předpokládat, že společenské normy reálného života, které nejsou běžné v celosvětové síti kyberprostoru, mohou být v něm také vyrovnány.

S přihlédnutím ke skutečnosti, že povaha kyberzločince a motivace jeho typické činnosti se utvářejí dvěma způsoby: reálným životem a kyberprostorem, je obzvláště důležitá skutečnost, že z reálného světa si kyberzločinec do kyberprostoru přenáší svůj kyberprostor. Poslední do značné míry v moderní společnosti je podmíněno vzestupem kultu spotřeby.

To vše vede k tomu, že kyberzločinec realizuje ve svém kyberprostoru model chování „pána života“ nebo běžně využívá kyberprostor k dosažení svých cílů v reálném životě – zisku a prospěchu.

Rozsah tohoto faktoru při determinaci kyberkriminality spočívá v tom, že se mezi dnešní mládeží vytváří určitý typ jedince s pokročilými potřebami, kteří žijí okamžikem a věří v uspokojení svých potřeb jakýmikoliv prostředky. Tito mladí lidé se zaměřují na rychlé dosažení úspěchu, mají určitou ochotu riskovat a smysl pro obchod. Nízká míra odhalování a zveřejňování kyberkriminality zároveň vede ke

[42] ERHARDT MUSTAINE, Elizabeth a Scott E. WOLFE. Cybercrime [online]. 1st century criminology a reference handbook. California: SAGE Publications, 2009 [cit. 2023-02-06]. 978–1 41296019.Dostupnéz:https://www.pravo.unizg.hr/_download/repository/21st_Century_Criminology__A_Reference_Handbook.pdf

vzniku mýtu o bezpečnosti těchto aktivit. To spolu s možností páchat tyto trestné činy bez ohrožení života vytváří další předpoklady pro to, aby se k páchání kyberkriminality dostávali stále noví a noví jedinci. Tomu napomáhá i popularizace a vykreslování kyberzločinců jako velmi slušných lidí nebo jakýchsi Robinů Hoodů bojujících proti „světovému zlu“ –vyspělým zemím a nadnárodním korporacím.

Sociální a psychologická fakta

Sociální a psychologická fakta. Jak známo, člověk je bytost sociální, a proto má velké znalosti pro internalizaci determinativního komplexu, tedy kriminálního chování, kriminogenních skutečností celého společenského řádu. Specifická povaha páchání kybernetické kriminality v mnoha případech určuje zvláštnosti psychické formace a pohledu na kyberprostor zločince.

Významnou roli při určování kyberkriminality hraje takový specifický psychologický faktor, jako je „online disinhibiční efekt“ (v terminologii Johna Sulera – vliv kyberprostoru na člověka, který mu umožňuje jednat svobodněji než v reálné společnosti. Umožňuje mu jednat svobodněji než v reálné společnosti). Základem tohoto efektu je:[43]

– *diskrétní anonymita* („neznáte mě“), jejíž podstatou je, že v podmínkách anonymity mohou lidé oddělit svou identitu v kyberprostoru od reálného světa a skutečné osoby, v takovém případě se osoba domnívá, že nemusí nést odpovědnost za své činy;[44]
– *neviditelnost* („nevidíš mě“) – umožňuje vyhnout se nutnosti navázat psychologický kontakt;
– *asynchronnost* („uvidíme se později“) – schopnost komunikovat v určitých případech bez nutnosti rychlé reakce na slova nebo činy partnera, což je důležitý demotivační prvek;
– solipsistické vniknutí („všechno je to v mé hlavě“) – možnost, že v online

[43] SABILLON, Regner, Jordi SERRA–RUIZ, Jeimy J. CANO M. a Víctor CAVALLER. Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security [online]. June 2016(4), 165–176 [cit. 2023–02–04]. ISSN 2410–0595. Dostupné z: www.ijcncs.org
[44] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 392. ISBN 978-80-7598-554-5.

komunikaci můžeme mít pocit, že se vše odehrává výhradně v naší vlastní představivosti;

– minimalizace moci („jsme si rovni“) – vyplývá z pociťované ztráty atributů vyššího společenského postavení také možné ji ignorovat. Je však nutné si uvědomit, že v kybernetická společnosti můžeme hovořit o zániku některých dalších, ale stále ještě hierarchií.

Viktimologické faktory

Faktory spojené s chováním obětí se projevují v nedostatku většiny populace v absenci náležité kultury bezpečného chování při používání počítačů, a to zejména v souvislosti s nedostatečnou úrovní chování obětí při manipulaci s počítačovým vybavením. Oběti zejména šetří peníze na softwarových a hardwarových ochranných systémech informací (nedostatek antivirového softwaru, firewallů; podceňování aktualizací softwaru ochrany; používání nelicencovaného softwaru), porušování obecných pravidel používání softwaru a jeho pravidel pro práci s informacemi v síti (absence záložních kopií důležitých informací, porušení anonymity, používání produkčního počítače k nevhodným účelům), ignorování požadavků na ochranu osobních údajů, které jsou v souladu se zákonem o ochraně osobních údajů (např. účelů), ignorování požadavků zaměřených na uchování důvěrných informací (nedostatek místních předpisů o používání počítačového vybavení v podniku, nedostatečný dohled nad pracovníky s přístupem k důležitým informacím, nedokonalý systém ochrany heslem proti neoprávněnému přístupu k pracovní stanici a jejímu programovému vybavení, - systém ochrany heslem proti neoprávněnému přístupu k pracovní stanici a jejímu programovému vybavení. Programové vybavení, které neumožňuje spolehlivou identifikaci uživatele podle jednotlivých osob biometrických parametrů), porušování dalších pravidel (chování veřejných osobních života), jakož i neoznámení kyberkriminality ze strany obětí.

Charakteristika této skupiny determinantů je důležité si uvědomit, že specifické prostředí kyberkriminality určuje také specifičnost vztahů na úrovni kyberzločinec-oběť trestného činu.

V podmínkách kyberprostoru se významně mění psychologický význam vztahu pachatel – objekt trestného činu i pachatel – oběť, které se přímo promítají do zkoumání: pachatel – elektronické zařízení (Síť) – oběť (objekt trestného činu), což vede ke stanovení materiální složky lidského i společenského jednání. Současně „virtuální“ předměty se z psychologického hlediska zdají být pro ostatní přístupnější, s výjimkou nelegálního držení. Jakékoli jednání je v takových podmínkách zpočátku vnímáno jako nehmotné, a proto nemá hmotné, závažné důsledky. Informační, mediální a komunikační technologie výrazně omezují zpětnou vazbu, jakýkoliv pocit zpětné vazby našeho jednání. Vliv má tedy vědomí, že jsme způsobili škodu, ale také přesvědčení, že naše chování žádnou škodu způsobit nemůže, protože ji nevidíme.

Specifická prostředí páchání kyberkriminality určuje také specifičnost vztahu mezi kyberzločincem a obětí trestného činu.

Diskrétní povaha a „virtualizace” škody způsobené jednáním realizovaným v kyberprostoru umožňuje specifické vnímání oběti trestného činu. Na jedné straně oběť trestného činu, která odhalí způsobenou škodu a „neuvědomí si ji”, plně neodráží metody a techniky, resp. povahu a stupeň závažnosti nebezpečnosti trestného činu. Na druhou stranu oběť trestného činu často není schopna adekvátně spojit újmu s pachatelem ve svém vlastním vědomí. Trestný čin spáchaný na oběti a jím způsobená újma jsou tak často obětí vnímány jako absolutní zlo, které nemá šanci na nápravu.

Pokud jsou si pachatel i oběť trestného činu vědomi nezákonnosti a společenskou nebezpečnost činu a jeho následky, je třeba zohlednit specifika vztahu na úrovni kyberzločince – oběti trestného činu určují následující skutečnosti. Jak upozorňují odborníci, paradoxním rysem kyberkriminality je těžké najít jiný druh trestného činu po kterém oběť neprojevuje velký zájem o dopadení pachatele, a pachatel po dopadení všemožně propaguje svou činnost v oblasti hackingu tají před orgány činnými v trestním řízení.

Psychologicky je tento paradox celkem pochopitelný. Za prvé, oběť kyberzločinu je naprosto přesvědčena, že náklady na jeho prozrazení (včetně ztrát

vzniklých v důsledku ztráty jeho dobrého jména) výrazně převyšují již způsobenou škodu. A za druhé, zločinec si získává širokou oblibu v obchodních a kriminálních kruzích, což mu dále umožňuje ziskové využití získaných zkušeností

Je třeba poznamenat, že se nejedná o vyčerpávající seznam příčin a podmínek (determinantů, faktorů) kyberkriminality, faktorů) kyberkriminality vzhledem ke složitosti příslušných společenských vztahů.

Stojí za zmínku, že v odborné literatuře někteří badatelé identifikují také tzv. kulturní faktory (podle nichž je páchání kyberkriminality, stejně jako jiných druhů trestné činnosti je spojena s negativními důsledky poklesu obecné kulturní a morální úrovně, a to zejména v souvislosti se snížením úrovně morálky a morálních hodnot kritérií ve společnosti) atd.

Intenzivní informatizace a globalizace světa proto při absenci účinných mechanismů ekonomické, politické a právní regulace (jak na úrovni jednotlivých států, tak i na mezinárodní úrovni) těchto procesů vede ke kriminalizaci značné části jejich součástí. Přitom čím nižší je úroveň ekonomického rozvoje země, politického a právního zajištění její informační bezpečnosti, tím vyšší je míra kybernetické kriminality a kybernetických hrozeb obecně.

Měli bychom se také shodnout s odborníky, že významné místo při určování kyberkriminality zaujímá psychologické procesy, k nimž dochází při přímém páchání trestné činnosti kyberkriminality. Na rozdíl od převážné většiny běžných trestných činů je spáchání trestného činu kybernetického trestného činu zpravidla nevyžaduje žádný pohyb či aktivního fyzického jednání. Kyberzločinec při realizaci svého zlého úmyslu je doma, v počítačovém klubu, na místě s volným přístupem k internetu nebo na jakémkoli jiném místě, kde se může dopustit jiném místě, které je mu příjemné nebo alespoň známé a důvěrně známé. Proto kyberzločinec nemusí pociťovat nebo v mnohem menší míře pociťuje nepříjemné pocity nebo strach z náhodného odhalení a zadržení. Kyberprostor je sice mnohotvárným sociálním prostorem, ale zároveň zůstává uměle vytvořeným softwarovým a hardwarovým prostředím, kde jsou aktivity stále omezeny technickými rámci, což činí důsledky jednání předvídatelnými. To zase umožňuje pachateli nepociťovat

nejistotu situace, plánovat své jednání i za nepříznivých okolností, a proto se při páchání trestné činnosti cítit jistěji a klidněji. Právě tyto rysy určují úmyslnou povahu kyberkriminality. Na druhé straně tyto rysy prostředí kyberkriminality by měly orgány činné v trestním řízení brát v úvahu při vývoji vhodných metod a praktickém provádění opatření k odhalování, potlačování, vyšetřování trestných činů této kategorie a prevenci jejich šíření.

Výše uvedené nám umožňuje konstatovat, že konkrétní rysy determinace kyberkriminality jsou podmíněny úlohou kyberprostoru jako média pro formování osobnosti pachatele, souboru vlastností, které existují nezávisle na osobě, kdo trestný čin spáchal (prostředí trestného činu, které určuje povahu trestného činu), a jeho vztah k relevantním skutečnostem reálného světa (sociální prostředí).

3.3. Charakteristika kyberzločince: typologie a klasifikace

Podezřelé osoby ze spáchání trestného činu a osobnost pachatele je jedním z hlavních součásti předmětu kriminologie a dává identifikovat všechny ostatní kriminologické problémy, ať už se jedná o determinanty kriminality nebo organizování boje proti ní. Představitelé klasických kriminologických škol věnovali značnou pozornost studiu osobnosti pachatele kriminologické školy. Například C. Beccaria, I. Bentham, F. List, L. Feuerbach a další vědci v XVIII –XIX století důrazně odmítl teologické chápání zločinu jako projevu "satanského", ďábelského počátku. Podle nich je zločinnost důsledkem vědomého jednání chování člověka, který má plnou svobodu vůle, rozhoduje o svém jednání.[45]

Moderní badatelé se dotýkají různých aspektů osobnosti zločince. Na základě z různých popisů, které jsem prostudovala o identitě kyberzločince, jsem dospěla k následujícím vlastním, závěrům ohledně popisu kyberzločince. Podle mého průzkumu jsou kyberzločinci většinou schopni, ale nezaměstnaní, svobodní

[45] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978–80–7598–554–5.

muži, jejichž morální a psychické vlastnosti ovládá sobectví, právní nihilismus v kombinaci s komplexem libovůle a iluzí.

Vzhledem k celkovému dalšímu růstu celkového počtů trestných činů počet a variabilita trestných činů s využitím počítačových sítí další kriminologických studie osobnosti kyberzločince jsou nyní relevantní.

Cílem tohoto oddílu je provést kriminologickou charakteristiku kyberzločinců na základě studia osob podezřelých ze spáchání trestných činů s využitím počítačů a také vytvořit typický portrét kybernetického podvodníka.

Nelze konkrétně popsat typ pachatele kyberzločinců: *„Z hlediska charakteristiky pachatele záleží vždy na druhu či typu trestné činnosti, které se dopouští, neexistuje typický pachatel kyberkriminality, předpokladem je pouze základní uživatelská znalost kyberprostoru“*[46]

Při zkoumání osob, které páchají trestnou činnost prostřednictvím kyberprostoru, mohou být je třeba posuzovat jak z hlediska charakteristik trestných činů, tak z hlediska charakteristiky osobnosti pachatele. Odborníci z Norwichské univerzity (soukromá vojenská univerzita v Northfieldu ve státě Vermont, USA) proto rozlišují následující typy trestných činů, USA), rozlišují následující typy kyberzločinců:

Zloději identity jsou obvykle kyberzločinci, kteří se snaží získat přístup k osobním údajům obětí (jméno, adresa, telefonní číslo, pracoviště, bankovní účet, informace o kreditní kartě a číslo sociálního pojištění) a tyto informace použít k finančním transakcím vydávajícím se za oběť;

Internetoví stalkeři jsou kategorií kyberzločinců, kteří zákeřně kontrolovat online aktivity svých obětí. Tato forma trestné činnosti je páchána prostřednictvím

[46] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 392. ISBN 978-80-7598-554-5.

sociálních médií a malwaru, který dokáže sledovat počítačové aktivity osoby s velmi malou mírou odhalení;

Phishing Scammers jsou kategorií kyberzločinců, kteří se snaží získat osobní nebo důvěrné informace prostřednictvím počítačů obětí, často prostřednictvím „phishingových“ webových stránek;

Kyberteroristé jsou dobře vyvinutou, politicky inspirovaná kategorie zločinců, jejíž členové se pokoušejí krádež dat a/nebo kompromitace podnikových nebo vládních počítačových systémů a sítí, což může způsobit škodu celým zemím, podniky, organizace nebo jednotlivci.[47]

Motivačními faktory pro kyberzločince jsou obvykle se označují jako: dosažení peněžního zisku; špionáž; sabotáž politického nebo náboženského přesvědčení; zvědavost; vyhledávání vzrušení, sexuální pudy; netolerance; zvyšování sebevědomí a záměr ovládat a manipulovat ostatní. Někdy je u tohoto typu pachatele diagnostikován narcismus a další psychopatie. R. Mitchell identifikoval typy kyberzločinců, kteří se liší úrovní svých dovedností a motivace: začátečníci, cyberpunk, interní (vnitřní hrozba); programátoři; informační bojovníci/kyberteroristé; staří bezpečnostní hackeři; profesionální kyberzločinci.[48]

3.4. Výsledky vlastního šetření

Za účelem provedení kriminologické charakteristiky kyberzločinců jsem provedla zkoumání s využitím zdrojů, které jsou veřejně dostupné na internetu v souvislosti se zločinci hledanými federální policií Úřadu pro vyšetřování (FBI) Spojených států amerických. Úplný seznam osob, které obsahující 117 podezřelých osob hledaných FBI pro podezření ze spáchání kybernetické trestné

[47] Who Are Cyber Criminals?. Norwich.edu [online]. norwich: Cybersecurity by Norwich University Online, February 13th, 2017 [cit. 2023-01-29]. Dostupné z: https://online.norwich.edu/academic–programs/resources/who–are–cyber–criminals

[48] Global Cyber Security Capacity Centre: Profiling the Cybercriminal [online]. Oxford, 18 April 2016n. l. [cit. 2023-02-01]. Dostupné z: https://gcscc.ox.ac.uk/article/profiling–cybercriminal

činnosti, je k dispozici na internetové stránce Webové stránky „Nejhledanější zločinci“.[49]

Podle výsledků průzkumu jsem odhalila sociálně významné rysy mezinárodního kyberzločince.

Podle věkového kritéria tak bylo zjištěno, že většina osob 60% na federálním a mezinárodním seznamu hledaných osob jsou ve věku přibližně 19 až 35 let a podle pohlaví jsou vyšetřovanými podezřelými z kyberkriminality muži. Tato skupina tvoří největší počet hledaných osob. Na rozdíl od obecné trestné činnosti je nepřítomnost osob ve věku 65 let a starších mezi odsouzené osoby ve věkové skupině 65 let a starší. To je způsobeno především tím, že většina lidí v této věkové skupině nemá odpovídající dovednosti pro práci s počítačovým vybavením a také díky jejich větším životním zkušenostem a vyšším morálním hodnotám. Je třeba poznamenat, že seznam kyberzločinců, který sestavila FBI zahrnuje skutečně obzvláště nebezpečné pachatele, kteří způsobili značné finanční škody společnostem nebo státu, narušili informační bezpečnostní systémy řady národních agentur a narušil provoz informačních technologií, ale většina z nich byly namířeny proti Spojeným státům americkým. Kromě toho, na seznamu nejsou žádní občané USA. Proto vyvozovat objektivní závěry z územních důvodů je velmi obtížné identifikovat kyberzločince podle území.

Na základě těchto údajů je však stále možné s určitou pravděpodobností potvrdit skutečnost, že většina zločinců jsou občané zemí s nízkou úrovní boje proti kyberkriminalitě, jako jsou země Blízkého a Dálného východu (Pákistán, Indie, Írán, Sýrie, Vietnam atd.)

Úroveň vzdělání je důležitým prvkem rysem sociodemografické charakteristiky pachatele, protože do značné míry určují jeho sociální status osoby, druh a kvalifikaci práce a obecně vypovídá o úrovni jejího intelektuální rozvoj a kultuře. O postojích k životu, životní orientaci, potřebách a zájmech, motivech a cílech činnosti, pravidlech chování, způsobech chování a jednání a

[49] Cyber’s Most Wanted: Select the images of suspects to display more information. FBI [online]. USA [cit. 2023-01-29]. Dostupné z: https://online.norwich.edu/academic–programs/resources/who–are–cyber–criminals

způsobech reakce na konkrétní životní situace. Čím vyšší je úroveň vzdělání jednotlivce, tím méně příležitosti k vytváření protispolečenských postojů, návyků a jejich kriminálních projevů. Nízká úroveň vzdělání usnadňuje výběr prostředků a způsobů realizace potřeby a touhy a volba kriminálního chování.

Obecně je známo, že kriminogenní význam má skutečnost, že práceschopný člověk nepracuje, nestuduje ani nevykonává jiné společensky prospěšné činnosti člověk zbavený legálního příjmu a prostředků k obživě, obklopený negativním mikroprostředím, se snadno a přirozeně vydává na kriminální dráhu. Na druhou stranu, jak ukazuje praxe, kyberkriminalita, s přihlédnutím k úrovni vzdělání pachatele a dalším sociodemografickým údajům je třeba charakteristiky, se dopouštějí zdaleka ne marginální, primitivní a kriminálně orientovaní lidé představitelé naší společnosti. Páchání kybernetické trestné činnosti navíc vyžaduje dostupnost potřebné technické (počítačové) vybavení nebo alespoň přístup k němu.

Proto podle mého názoru příslušné statistiky ukazují, že domácí pracovněprávní, daňová a jiná legislativa a její aplikační praxe jsou nedokonalé pracovněprávní, daňové a jiné právní předpisy a praxe jejich uplatňování, které umožňuje příslušné kategorii osob „usadit se“ ve společnosti, oficiálně mít status nezaměstnaného atd.

Jedním z nejdůležitějších ukazatelů, který charakterizuje morální úroveň člověka pachatele je jeho postoj k alkoholismu a drogové závislosti. Analýza statistických údajů ukázal, že kyberzločinci (na rozdíl od většiny zločinců) se vyznačují tím, že páchají trestné činy výhradně ve střízlivém stavu. Existuje zatím pouze jediný případ odsouzení za spáchání počítačové trestné činnosti pod vlivem alkoholu. To potvrzuje závěr kriminální zaměření osobnosti kyberzločince, který se dopustil trestného činu chladnokrevně a pečlivě, čímž dosáhl předvídatelného výsledku.

Na základě analýzy statistických údajů nebylo zjištěno, že by se žádná osoba dopustila příslušný čin ve stavu nepříčetnosti nebo omezené příčetnosti.

Osobní odchylky jsou bohužel téměř vždy přehlíženy jsou bohužel téměř vždy ignorovány vyšetřováním a soudem vzhledem k závažnosti trestného činu tohoto druhu trestné činnosti a nedostatek příslušných odborných znalostí.

Co se týče intelektuálních charakteristik kyberzločince, povaha počítačových trestných činů vyžaduje zjištění určitých vlastností obviněného, pokud jde o technické znalosti, jejich vlastnosti a intelektuální schopnost spáchat trestný čin. To znamená je vyžadována odpovídající intelektuální úroveň člověka, spojená se schopností správně pochopit a použít pokyny atd.

Někteří odborníci poukazují na to, že charakteristickým rysem počítačových zločinců je dostatečně vysoká intelektuální úroveň pachatele, neboť spáchání trestného činu vyžaduje složité operace, zejména psaní počítačových programů, volbu hesel přístup k bezpečnostním systémům, schopnost převzít na sebe elektronickou činnost vyžaduje nejen speciální znalosti a dovednosti, ale také dostatečně vysokou úroveň sebevědomí, kontroly nad sebou samým a situaci, v níž byl trestný čin spáchán. V některých případech totiž spáchání kybernetického trestného činu vyžaduje značnou psychickou zátěž, úsilí a vážné dobrovolné soustředění, nicméně z našeho pohledu je takové tvrzení nelze brát kategoricky. Ačkoli na rozdíl od osob, které se dopouštějí trestných činů obecného charakteru se kyberzločinci vyznačují vysokou úrovní vzdělání, vyšším vzděláním a vyšší úrovní než úroveň vzdělání obyvatelstva, ale v souladu se sociálním postavením a dalšími sociálními a společenskými podmínkami demografické charakteristiky, kyberzločinci odrážejí strukturu populace jako celku. V důsledku toho přiměřená úroveň intelektuálního rozvoje kyberzločince není konstantou, ale předmětem prokázání schopnosti (možnosti) konkrétní osoby spáchat příslušný čin.

Motivace kyberzločinců.

Kriminologická podstata trestného činu a tedy i osobnostní stránka osoby, která ji páchá, se nejplněji projevuje v obsahu motivace k trestné činnosti, protože je to motivace, která nevyjadřuje žádný individuální osobnostní rys, ale v určitém smyslu celý člověk, všechny jeho charakteristické vlastnosti a rysy. Motiv stmeluje myšlenku a vůli, vědomí a jednání a slouží jako hlavní pramen, který řídí proces

vůle, dává mu určitý obsah. Motiv je tedy jedním z nejvýznamnějších psychologických faktorů pojmy, které odhalují vnitřní povahu lidského jednání, jeho podstatu. Je nejdůležitější složkou psychické struktury každého člověka. činnost, její hnací síla, označuje vnitřní (psychologický) důvod jednání člověka konkrétní osoby.[50]

Shrneme-li výše uvedené, můžeme říct, že osoba kyberzločince je mezinárodním společenstvím vnímána v širokém smyslu. Často jednají sami, někdy se organizují do malých skupiny, které se vyznačují rozdělením rolí a zvýšeným nebezpečím, protože jsou mnohem efektivnější. Usilují o neustálé zlepšit své dovednosti a schopnosti. Pro větší význam pro ně mají intelektuální úspěchy a překonávání obtížných překážek a překonávání obtížných překážek jsou pro něj důležitější než hmotné zisky.

Závěrem bych chtěl upozornit na skutečnost, že představený profil kyberzločinců rozhodně nevyčerpává celé spektrum kyberzločinců těchto jedinečných jedinců, ale může to být jeden z kroků ke komplexnímu kroky ke komplexní studii této problematiky.

[50]Digital forensics investigation of internet of things (IoT) devices. Editor Reza MONTASARI, editor Hamid JAHANKHANI, editor Richard HILL, editor Simon PARKINSON. Cham: Springer, [2021]. Advanced sciences and technologies for security applications. ISBN 978–3–030–60424–0.

Závěr

Vytvoření aktuální politiky kybernetické bezpečnosti a zajištění účinnosti jejího provádění, fungování bezpečného kyberprostoru, jakož i prevence a potírání kyberkriminality patří v současné fázi vývoje společnosti k nejnaléhavějším úkolům a výzvám pro státy a mezinárodní společenství. Proto je studium některých otázek kybernetické bezpečnosti předmětem výzkumu vědců z různých oborů.

V kriminologii je kybernetická bezpečnost vnímána jako souhra jednotlivých složek: státní politiky v oblasti kybernetické bezpečnosti; aktérů kybernetické bezpečnosti; prostředků, způsobů a metod zajištění kybernetické bezpečnosti. Jednou z klíčových hrozeb kybernetické bezpečnosti je zejména kyberkriminalita.

Přestože je kyberkriminalita a kybernetická trestná činnost předmětem studia stále většího počtu moderních vědců, existují určité obtíže při studiu tohoto společenského jevu, což ve svém důsledku zpomaluje fungování systému kybernetické bezpečnosti na národní i mezinárodní úrovni, neboť ten se formuje na základě teoretického výzkumu. Podle mého názoru hlavních problematických otázek jsou:

Za prvé, v právní doktríně a pracích domácích i zahraničních vědců neexistuje jednotný přístup k terminologii.

Za druhé, nesoulad stávajících právních předpisů s mezinárodními normami.

Za třetí, kriminologický výzkum způsobů páchání kyberkriminality je omezený.

Na základě výše uvedeného lze konstatovat, že pod vlivem nekontrolovaného využívání kyberprostoru s vzhledem k délce četnosti a intenzitě konzumace informací, která je spotřebitelům často vnucována, dochází k výrazné deformaci jedince, jeho morálních a psychických vlastností. Vzhledem k intenzitě rozvoje globálního informačního prostoru je nutné provádět nejen základní kriminologický výzkum, ale také soustavný „kriminologický monitoring“

informačního kyberprostoru, počítačových sítí, který je možný v rámci speciální kriminologické teorie.

Seznam použité literatury

Monografie

GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 390-407 ISBN 978-80-7598-554-5.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. s. 74-148. ISBN 978-80-88168-15-7

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

MAREŠ, Petr. Kyberkultura, hackeři a digitální revoluce: informace chce být svobodná. Praha: Grada, 2022. ISBN 978-80-271-3358-1.

VLACH, Jiří, Kateřina KUDRLOVÁ a Viktorie PALOUŠOVÁ. Kyberkriminalita v kriminologické perspektivě. Praha: Institut pro kriminologii a sociální prevenci, 2020. Studie (Institut pro kriminologii a sociální prevenci). ISBN 978-80-7338-189-9.

TENCH, Ralph a Liz YEOMANS. Exploring Public Relations 2nd Edition: Pearson; 2nd edition. Public Relations. January 1, 2009. ISBN 0273715941.

YOUNG, Suzanne a Katie STRUDWICK. Teaching Criminology and Criminal Justice: Challenges for Higher Education. Palgrave Macmillan, 2022. ISBN 978-3-031-14898-9.

Časopisecké články

ŠŤASTNÝ, Mgr. Bc. Jakub. Trestní postih DoS/DDoS útoků. EPRAVO.CZ – Sbírka zákonů, judikatura, právo [online]. 20. 4. 2020 [cit. 2023-03-07]. Dostupné z: https://www.epravo.cz/top/clanky/trestni-postih-dosddos-utoku-110941.html

International Journal of Cyber Criminology [online]. 2020 [cit. 2023-02-13]. ISSN 0974 - 2891. Dostupné z: http:// www.cybercrimejournal.com. [online]. [cit. 2023-02-01].

SABILLON, Regner, Jordi SERRA-RUIZ, Jeimy J. CANO M. a Víctor CAVALLER. Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security [online]. June 2016(4), 165-176 [cit. 2023-02-04]. ISSN 2410-0595. Dostupné z: www.ijcncs.org

Konferenční příspěvky

GHAFIR, Ibrahim a Václav PŘENOSIL. Advanced Persistent Threat and Spear Phishing Emails. In Miroslav Hrubý. Proceedings of International Conference Distance Learning, Simulation and Communication. první vydání. Brno, Czech Republic: University of Defence, 2015. s. 34-41. ISBN 978-80-7231-992-3.

Webové stránky a elektronické zdroje

ANDRESS, Jason a Steve WINTERFELD. Cyber Warfare.: Hacktivist [online]. 2016, 207 219 [cit. 2023-01-31]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/hacktivist

Black hat, White hat, and Gray hat hackers – Definition and Explanation. Kaspersky [online]. 2023 [cit. 2023-02-01]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

CREWS, Gordon A. Wiley Online Library: Determinism. Wiley Online Library [online]. 26 March 2014 [cit. 2023-02-05]. Dostupné z: https://onlinelibrary.wiley.com/

Cross-site scripting (XSS) [online]. [cit. 2023-02-22]. Dostupné z: https://www.enisa.europa.eu/, KirstenS. Cross Site Scripting (XSS) [online]. [cit. 2023-02-01]. Dostupné z: https://owasp.org/www-community/attacks/xss/

Cyber's Most Wanted: Select the images of suspects to display more information. Fbi [online]. USA [cit. 2023-01-29]. Dostupné z: https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals

DIFFERENTIAL ASSOCIATION THEORY: SUTHERLAND'S SOCIOLOGY AND CRIMINOLOGY OF DEVIANCE EXPLAINED [online]. [cit. 2023-02-06]. Dostupné z: https://criminologyweb.com/differential association theory- sociology and crimi nology-of-deviance-explained/

DIGITAL 2022: OCTOBER GLOBAL STATSHOT REPORT [online]. 20 OCTOBER 2022n. l. [cit. 2023-02-01]. Dostupné z: https://datareportal.com/reports/digital-2022-october-global-statshot

DJERF-PIERRE, Monika. Squaring the Circle: public service and commercial news on Swedish television 1956?99. Journalism Studies [online]. 2000, 1(2), 239-260 [cit. 2023-01-29]. ISSN 1461-670X. Dostupné z: doi:10.1080/14616700050028235

ERHARDT MUSTAINE, Elizabeth a Scott E. WOLFE. Cybercrime [online]. 1st century criminology a reference handbook. California: SAGE Publications, 2009 [cit. 2023-02-06]. 978-1-4129-6 019. Dostupné zhttps://www.pravo.unizg.hr/_download/repository/21st_Century_Criminology__A_Reference_Handbook.pdf

Global Cyber Security Capacity Centre: Profiling the Cybercriminal [online]. Oxford, 18 April 2016n. l. [cit. 2023-02-01]. Dostupné z: https://gcscc.ox.ac.uk/article/profiling-cybercriminal

High Technology Crime Law and Legal Definition. Uslegal [online]. [cit. 2023-02-28]. Dostupné z: https://definitions.uslegal.com/h/high-technology-crime/

History: UNIVAC I. Census [online]. Eckert-Mauchly Laboratory in Philadelphia, PA, June 14, 1951 [cit. 2023-02-06]. Dostupné z: https://www.census.gov/history/www/innovations/technology/univac_i.html

Internet věcí používá v Česku třetina firem. Čidla mohou být ale terčem hackerských útoků. Tematický speciál E15 [online]. [cit. 2023-03-07]. Dostupné z: https://www.e15.cz/tematicke-specialy/kyberneticka-bezpecnost/internet-veci-pouziva-v-cesku-tretina-firem-cidla-mohou-byt-ale-tercem-hackerskych-utoku-1392728

K., Jaishankar. Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology [online]. 2018. – January–June. – Vol. 12 [cit. 2023-02-13]. Dostupné z: https:// pdfs.semanticscholar.org/4146/e6a16b448d63d476fce0a3a 81554b1852438 pdf.

KATZ Šimon. Kyberkriminalita – kriminologické aspekty [online]. Praha 2022. Bakalářská práce. Policejní akademie České Republiky v Praze Fakulta bezpečnostně právní. Vedoucí práce Mgr. Najman Tomáš [cit. 2023-02-11]. Dostupné z: https://theses.cz/id/vqqmn7/P_Kyberneticka_kriminalita.pdf

Kolda Ondřej. 7 black hat SEO technik, kterým se raději obloukem vyhněte [online]. 23. 07. 20210 [cit. 2023-03-07]. Dostupné z: https://www.blueghost.cz/clanek/7-black-hat-seo-technik-kterym-se-radeji-obloukem-vyhnete/

Kyberkriminalita. Odbor prevence kriminality Ministerstva vnitra [online]. [cit. 2023-02-06]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

KYBERKRIMINALITA: Jednotlivé druhy kyberkriminality. Policie České republiky [online]. [cit. 2023-01-31]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Mobile Threat Landscape 2020: Understanding the key trends in mobile enterprise security in 2020 [online]. 2020, 13 [cit. 2023-01-31]. Dostupné z: http://go.wandera.com/rs/988 EGM 040/images/Mobile%20Threat%20Landscape%202020.pdf

MUELLER, Annie. Famous White-Hat Hackers [online]. [cit. 2023-01-31]. PAKHOTA, N. V. Information Wars in Modern International Relations. Business Inform [online]. 2022, **1**(528), 53-58 [cit. 2023-02-01]. ISSN 22224459. Dostupné z: doi:10.32983/2222-4459-2022-1-53-58

MUELLER, Annie. Famous White-Hat Hackers [online]. In: Updated July 16, 2022 [cit. 2023-02-01]. Dostupné z: https://www.investopedia.com/financial-edge/0811/famous white hat hackers.aspxHttps://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_ budapest_/7_conv_budapest_en.pdf.

Národní úřad pro kybernetickou a informační bezpečnost – Sociální inženýrství 2016. [online]. [cit. 2023-03-06] Dostupné z: https://nukib.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/

Policie ČR: PREVENTIVNÍ INFORMACE. Vishing a spoofing [online]. [cit. 2023-03-01]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

Policie ČR: Vývoj registrované kriminality v roce 2022 [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

SCHEINOST, PhDr. Miroslav a JUDr. Zdeněk KARABEC, CSC. Zneužití identity a trestná činnost s tím spojená. Institut pro kriminologii a sociální prevenci, Praha [online]. [cit. 2023-03-07]. Dostupné z: https://www.mvcr.cz/soubor/scheinostkarab-identity-pdf.aspx¨

Software Management: Security Imperative, Business Opportunity: 2018 BSA GLOBAL SOFTWARE SURVEY [online]. 2018 [cit. 2023-02-01]. Dostupné z: https://gss.bsa.org/

The Economic Impacts Of Cyber Crime: How It Costs Us All. Cyber security [online]. 30 June 2022 [cit. 2023-02-05]. Dostupné z: https://mitigatecyber.com/the-economic-impacts-of-cyber-crime-how-it-costs-us-all/

Understanding the key trends in mobile enterprise security in 2020 [online]. [cit. 2023.01 31]. Dostupné z: http://go.wandera.com/rs/988 EGM 040/images/Mobile %20Threat%20Landscape%202020.pdf

United Nations Office on Drugs and Crime: The United Nations Congress on Crime Prevention and Criminal Justice [online]. 2021 [cit. 2023-01-29]. Dostupné z: https://www.unodc.org/unodc/en/crimecongress/about.html

What is Spoofing – Definition and Explanation [online]. [cit. 2023-02-28]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/spoofing

Who Are Cyber Criminals? [online]. Norwich [cit. 2023-01-29]. Dostupné z: https://online.norwich.edu/academic programs/resources/who are cyber criminals

WikiSofia: Digitální propast. Definice digitální propasti, základní dimenze digitální propasti, demografické skupiny nejvíce ohrožené digitální propastí ve vyspělém světě [online]. Univerzita Karlova v Praze, Filozofická fakulta, 2013-2017 [cit. 2023-02-07]. Dostupné z: https://wikisofia.cz/

Wiley Online Library [online]. 26 March 2014 [cit. 2023-02-05]. Dostupné z: https://doi.org/10.1002/9781118517390.wbetc022

YAR, Majid. The Novelty of ‘Cybercrime’. European Journal of Criminology [online]. 2005, 2(4), 407-427 [cit. 2023-01-29]. ISSN 1477-3708. Dostupné z: doi:10.1177/147737080556056

Legislativní zdroje

Úmluva Rady Evropy č.185 o kybernetické kriminalitě ze dne 23.11.2001 [online]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104/zneni-20190705

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů [online]. [cit. 2023-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181