Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra systémového inženýrství

Bakalářská práce

Kyberkriminalita z pohledu systémové dynamiky

Alena Pejčochová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Bc. Alena Pejčochová, M.A.

Systémové inženýrství a informatika
Informatika

Název práce

Kyberkriminalita z pohledu systémové dynamiky

Název anglicky

Cybercrime from a System Dynamics Point of View

Cíle práce

Cílem bakalářské práce je analýza vývoje kybernetické kriminality v České republice pomocí principů a nástrojů systémové dynamiky. Pro dosažení tohoto cíle bude sestaven a otestován simulační model.

Metodika

Bakalářská práce nejprve popíše teoretická východiska. Budou zhodnoceny vybrané aspekty kybernetické kriminality zaměřené na dynamiku vývoje a vazeb, od definice, typů, vymezení a projevů, až po analýzu zúčastněných aktérů podílející se na procesu prevence, odhalování a vyšetřování kyberkriminality v České republice. Dále bude na teoretické úrovni představena metoda systémové dynamiky. Na tuto část pak naváže praktická část zaměřující se na užití metody systémové dynamiky ke zkoumání problému kybernetické kriminality. Bude vytvořen simulační model kyberkriminality v České republice znázorňující vývoj systému během určitého časového úseku. Pomocí tohoto modelu budou simulovány různé scénáře možného vývoje. V závěru práce dojde k zhodnocení modelu včetně zhodnocení samotné aplikace systémové dynamiky.

Doporučený rozsah práce

30-40 stran

Klíčová slova

kybernetická kriminalita, kyberbezpečnost, systémová analýza, IT, model

---

Doporučené zdroje informací

KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. 522 s.

MILDEOVÁ, Stanislava – VOJTKO, Viktor a kol. (2008): Systémová dynamika. Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2008. ISBN 978-80-245-1448-2, 150 s.

POLČÁK, Radim a Tomáš GŘIVNA. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN: 978-80-903786-7-4, 220 s.

SALIM,H.M.(2014).Cybersafety: A systems thinking and systems theory approach to managing cyber security risks. PhD thesis, Massachusetts Institute of Technology.

SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, 636 s.

STERMAN, J. Business dynamics : systems thinking and modeling for a complex world. Boston: McGraw-Hill, 2000. ISBN 007238915. 982 s.

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Igor Krejčí, Ph.D.

Garantující pracoviště

Katedra systémového inženýrství

Elektronicky schváleno dne 30. 3. 2020

doc. Ing. Tomáš Šubrt, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 4. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 04. 10. 2020

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Kyberkriminalita z pohledu systémové dynamiky" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 28.11.2020

Poděkování

Velice ráda bych touto cestou poděkovala vedoucímu práce Ing. Igoru Krejčímu, Ph.D. za jeho ochotu, cenné připomínky na vysoce odborné úrovni a často i morální podporu při vedení této práce.

Kyberkriminalita z pohledu systémové dynamiky

Bakalářská práce se zabývá analýzou kyberkriminality v České republice z využitím principů a nástrojů systémové dynamiky. Práce staví na teoretickém zpracování první části, ve které se zabývá fenoménem kyberkriminality a shrnuje teoretická východiska systémové dynamiky. V praktické části pak aplikuje metodu systémové dynamiky na problém kyberkriminality tím, že nejprve představí obecný příčinně smyčkový diagram (causal loop diagram, CLD) zobrazující zúčastněné entity a vztahy mezi nimi. Na jeho základě pak zpracuje diagram stavu a toků (stock and flow diagram, SFD), který je základem pro počítačovou simulaci, která je nejprve otestována na reálných dostupných datech a poté představí predikce vlivu zvolených proměnných v určitém časovém úseku (do roku 2030). Závěrem práce bude aplikace systémové dynamiky zhodnocena a budou navržena doporučení ke zlepšení současného stavu kyberkriminality v České republice.

Klíčová slova: kyberkriminalita, kyberbezpečnost, systémová analýza, IT, model, diagram, systém, počítačová simulace, problém, systémová dynamika

Cybercrime from a System Dynamics Point of View

This thesis focuses on the analysis of cybercrime in the Czech Republic from the point of view of the principles and tools of system dynamics. The thesis presents a theoretical literature review in the first part, which deals with the phenomenon of cybercrime and summarizes the theoretical background of system dynamics. In the practical part, the method of system dynamics is applied on the problem of cybercrime. All the factors and relations between them are displayed in a general system causal loop diagram. Based on the information from the diagram a stock and flow diagram was build. The stock and flow diagram serves as a base for a computer simulation which has been validated by real world data and then presents assumptions about the influence of selected variables within a certain period of time (until 2030). The thesis concludes with an evaluation of the application of system dynamics methods and recommendations are proposed to improve cybercrime situation in the Czech Republic.

Keywords: cybercrime, cybersecurity, system analysis, IT, model, diagram, system, computer simulation, problem, system dynamics

Obsah

Seznam obrázků a tabulek

Seznam použitých zkratek

CLD – Casual loop diagram
SFD – Stock and flow diagram
NÚKIB – Národní úřad pro kybernetickou bezpečnost
NCOZ – Národní centrála organizovaného zločinu
PČR – Policie České republiky
ČSÚ – Český statistický úřad
ICT – Informační a komunikační technologie

1 Úvod

Ačkoliv ještě několik let zpátky nebyla kyberkriminalita ani vykazována v oficiálních statistikách Policie ČR, za poslední roky došlo k nabytí jejího významu a zvýšení zájmu o faktory, které ovlivňují její nárůst, odhalování a potlačování. Tento zájem lze připisovat nárůstu případů, které se jako kyberkriminalita označují a to především s ohledem na rozvoj internetu, kdy dochází k čím dál častějšímu přesouvání běžných lidských činností do kyberprostoru. V souvislosti s aktuální pandemií, je tento trend ještě znatelnější, jelikož výkon zaměstnání se často přesouvá do tzv. „homeofficů“ a vzhledem k zákazu prodeje v kamenných obchodech (a blížícím se svátkům) narůstá počet nákupů zboží online a tak nejen Interpol, ale také české úřady bijí na poplach kvůli rapidnímu nárůstu počtu bezpečnostních incidentů. Od doby, kdy je kyberkriminalita evidována, je znatelný její nárůst, stejně tak jako nárůst počtu uživatelů online a počtu bezpečnostních incidentů online. Vzhledem k tomu, že proces vzniku, oznamování a objasňování kyberkriminality je vzájemně provázán, byla k jeho zkoumání a simulaci možného vývoje v bakalářské práci použita metoda systémové dynamiky. Tato je ideální především s ohledem na to, že umožňuje zabývat se komplexními systémy a jejich chováním a vývojem v průběhu času za účelem odhalit proměnné mající v celém systému vliv, případně odhalit proměnné, při jejichž změně by mělo dojít ke zlepšení současného stavu.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem bakalářské práce je analýza vývoje kyberkriminality na základě modelů systémové dynamiky zachycujících pomocí principů a nástrojů systémové dynamiky kyberkriminalitu v České republice, konkrétně faktory podílející se na jejím vzniku, oznamování a práce orgánů činných v trestním řízení (se zaměřením na Policii ČR). Nejprve bude sestaven příčinně smyčkový diagram a vybrána specifická část problému k hlubší analýze formou diagramu stavů a toků. Oba modely budou představeny v grafické podobě, kdy k převodu diagramu na simulační model bude použit program Vensim® PLE for Macintosh 8.1.2 Double Precision x64.

2.2 Specifické cíle práce

Dílčí cíle práce byly definovány s ohledem na plnění zadaného cíle práce. Mezi hlavními body, které byly v rámci těchto cílů identifikovány a které slouží jako základ pro zpracování metodiky práce patří:

1. Grafické vyjádření a popis vazeb zpracovávaného systému v rámci vytýčených hranic modelu
2. Sestavení CLD modelu zachycujícího dynamiku systému kyberkriminality v ČR
3. Popis struktury systému a identifikace kritických oblastí
4. Sestavení SFD modelu zaměřeného na konkrétní část systému
5. Testování modelu SFD pomocí porovnání výsledků simulace a reálných dat
6. Simulace scénářů se zvolenými parametry včetně citlivostní analýzy změny vybraných parametrů
7. Interpretace výsledků provedených simulací
8. Návrhy a doporučení ke zlepšení stávajícího stavu

2.3 Metodika

Základem zpracování práce je studium a analýza odborné literatury a dostupných zdrojů, tedy nejen tuzemských a zahraničních akademických zdrojů, ale také dosud akademicky nezpracovaných témat, která jsou však aktuální. Teoretická oblast zkoumání je nejen z oblasti kyberkriminality, ale také z oblasti systémové dynamiky. K úspěšnému

sestavení simulačního modelu je rovněž nezbytné si osvojit základní principy systémové dynamiky a poznatky z dokumentace k programu Vensim.

Dále budou formou CLD diagramu zobrazeny hlavní prvky systému podílející se na procesu odhalování a objasňování kyberkriminality. Následně budou identifikovány a okomentovány stěžejní zpětnovazební smyčky. Ačkoliv byl diagram stavů a toků sestavován postupně, s ohledem na rozsah práce bude znázorněna pouze jeho finální podoba. Diagram bude sloužit jako podklad ke zvolení specifického problému k sestavení SFD, tím, že definuje hranice modelu a zachycení vztahů mezi proměnnými.

Jako vstupní data pro simulační model pak slouží data veřejně dostupná na webových stránkách Českého statistického úřadu, Policie ČR a z dalších relevantních zdrojů.

Přesnost predikce simulačního modelu bude ověřena pomocí testovací simulace pro období 2011 – 2019 (s ohledem na dobu statistického vykazování kyberkriminality). Simulované výsledky budou vyhodnoceny s využitím průměrné procentuální chyby odhadu - Mean Absolute Percentage Error (MAPE).

Období simulace bylo zvoleno do roku 2030, kdy počáteční stavové hodnoty budou nastaveny na hodnoty v roce 2011. Změna proměnných však bude nastavena tak, aby se projevila až od roku 2019. V rámci simulace budou sestaveny různé scénáře a jejich dopady testovány funkčním modelem. Dále bude provedena analýza výsledků simulace a návrh doporučení ke zlepšení současného stavu.

3 Teoretická východiska

3.1 Fenomén kybernetické bezpečnosti a kybernetické kriminality

3.1.1 Kyberprostor jako prostor k páchání trestné činnosti

Internet byl vyvinut před desítkami let pro vojenské účely, ale zcela změnil způsob, jakým dnes žije globální populace. Tato síť se později stala páteří „kyberprostoru“ - virtuální reality bez hranic, dynamickým, neustále se měnícím a vyvíjející systémem, který vzniká jako určitý virtuální prostor paralelně s tím fyzickým. Je obecně vnímán jako „nehmotný“, nicméně stále vázán na hardware a tedy i obecně vnímaná „anonymita“ a „nedostižitelnost“ pachatelů je naštěstí (z pohledu Policie ČR) pouhou klamnou představou, ačkoliv možnosti odhalování pachatelů jsou, na rozdíl od fyzického světa, často komplikované. Každý den narůstá počet osob, které jsou připojeny online, zároveň také narůstá počet činností, které se do této sféry přesouvají. Aktuálně je tento vývoj ještě umocněn globální pandemií, kdy se aktivity cíleně přesouvají do kyberprostoru, jelikož je omezena dříve běžná možnost fyzického kontaktu (a to jak v soukromé, tak v podnikatelské sféře). Nejen v českých médiích se objevují zprávy o alarmujícím nárůstu kybernetických incidentů (Husák, 2020), ale také Interpol ve své zprávě ze srpna 2020 (Interpol, 2020) uvádí narůstající počty útoků nejen na státní úřady, kritickou infrastrukturu, ale také na jednotlivce – dochází například k zasílání podvodných SMS zpráv i e-mailů informujících o výsledku testování (Zoulová, 2020) – a malé a střední firmy překotně se snažící umožnit práci z domova během pandemie Covid-19. Kyberprostor se neustále a rychle rozvíjí a stále více zahrnuje aspekty života běžných lidí, takže existuje mnoho snah o zajištění jeho větší bezpečnosti. Pachatelé na jedné straně, a specialisté ze soukromé a státní sféry na druhé, se každý den v kyberprostoru „utkávají“, až může svým způsobem připomínat bojiště. Toto se však podstatně od bojišť minulosti liší především tím, že protivník může během několika sekund zaútočit na druhé straně světa a zároveň na několika místech najednou. Navíc mezi kybernetické incidenty lze (ne však v této práci) též řadit i ty, které nejsou úmyslné. Mohou být jednoduše způsobeny nesprávným fungováním technologií, neúmyslným lidským selháním, přírodními katastrofami apod. Jakákoliv opatření proti neúmyslným incidentům jsou pak samozřejmě využitelná i pro obranu proti případům úmyslných útoků.

3.1.2 Kybernetická bezpečnost a bezpečnostní incidenty

Kyberprostor je stále mnohými vnímán jako „bezpečné prostředí“, ve kterém jsou sdíleny informace. Včetně těch, kterými jsou ovládány předměty ve fyzickém světě, ačkoli krádež identity nebo krádež citlivých dat prostřednictvím informačních technologií a sociálních sítí je opakujícím se jevem. Oběťmi se pak stávají jednotlivci i společnosti.[1] Soukromé společnosti a vlády shromažďují velké množství dat, která ukládají, třídí a analyzují, což vždy představuje hrozbu. V případě „velkých hráčů“ by dokonce mohli představovat hrozbu pro demokracii.[2] Jako bezpečnostní incident, kterým byla ohrožena data nejvíce uživatelů je považován útok na Adobe v roce 2013, při kterém bylo odcizeno odhadem 3 miliony šifrovaných záznamů s údaji o kreditních kartách zákazníků, průkazů totožnosti, hesel a asi 150 milionů přihlašovacích údajů aktivních uživatelů (Swinhoe, 2020). Ani úřady státní správy se takovým incidentům nevyhýbají, jako v případě získání přístupu k vládním počítačům amerického Úřadu pro personální management, které obsahovaly 21,5 milionů záznamů nejen vládních zaměstnanců, ale také žadatelů a držitelů bezpečnostních prověrek (Swinhoe, 2020). Správná bezpečnostní ochrana znamená vysoké standardy a může být velmi nákladná (již dnes existuje velký počet pojišťovacích společností v oblasti kybernetické bezpečnosti a tvorby podkladů pro ohodnocení rizik) a ačkoliv mnoho společností již opatření zajišťující dodržování kybernetické bezpečnosti implementuje, stále existuje velké množství společností a jedinců, kteří odmítají investice do bezpečnosti kvůli latentní povaze hrozby a pod dojmem, že neexistuje nic, co by pachatel mohl chtít.

Zpráva o stavu kybernetické bezpečnosti Národního úřadu pro kybernetickou bezpečnost za rok 2019 jako první bod uvádí, že rok 2019 se vyznačoval nárůstem počtu kybernetických útoků proti institucím, organizacím a firmám v České republice, kdy zároveň rostla závažnost incidentů (NÚKIB, 2020). Důležitým prvkem kybernetické bezpečnosti je s ohledem na zvyšující se digitalizaci přijímání opatření k ochraně kritické infrastruktury. Tato je totiž často v soukromém vlastnictví, kdy zahrnuje sektor finančnictví, veřejných služeb (voda, ropa, plyn, elektřina), dopravy, veřejného zdraví a bezpečnosti,

[1] 116 čísel údajů o bezpečnostních incidentech a další relevantní statistiky jsou dostupné na stránce https://www.upguard.com/blog/data-breach-statistics

[2] Existují také případy bezpečnostních incidentů, za kterými nebyl protiprávní úmysl. Například Twitter umožnil přístup k 330 milionům hesel v nezabezpečeném logu, kdy však nebylo zjištěno jejich neoprávněné použití. Tyto však (i s ohledem na definici bezpečnostních incidentů ČSÚ) nejsou v modelu uvažovány.

telekomunikací, potravinářství včetně zemědělství atd. Co se týče systémů spadajících pod zákon o kybernetické bezpečnosti (tedy těch, které jsou nezbytné pro chod státu evidoval NÚKIB v roce 2018 celkem 164 incidentů a v roce 2019 již 217 (NÚKIB, 2020). Europol ve své zprávě o hodnocení hrozeb organizované trestné činnosti z internetu (Europol, 2020) uvádí, že třetina členských států EU nahlásila případy útoků na kritickou infrastrukturu, nejčastěji se jednalo o malware nebo DDoS útok (například případ ochromení sítě vlaků ve Švédsku v důsledku útoku na dva švédské poskytovatele internetových služeb). V rámci EU pak byla přijata opatření k ochraně veřejné infrastruktury například formou výzkumných projektů financovaných 7. rámcovým programem pro výzkum a technologický rozvoj, zřízením Výstražné sítě kritické infrastruktury (CIWIN) nebo přijetím Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Europol, 2019), ačkoliv se směrnice soustředí především na odvětví energetiky a dopravy. Ochrana kritické infrastruktury pak souvisí s obecnou ochranou dodavatelských řetězců, jejichž digitalizace je také náchylná ke kybernetickým útokům. Lze očekávat, že kybernetické útoky se budou stále více zaměřovat na nedostatečně chráněné dodavatelské sítě, kdy pachatelé budou motivování buď finančními, politickými nebo ideologickými cíli.

Soukromí a ochrana osobních údajů rovněž silně závisí na kybernetické bezpečnosti. Přijímaná opatření k ochraně dat jsou tak důležitá i pro bezpečnost (například šifrování, řádná správa osobních údajů, atd.). Jedním ze základních principů je, že „osobní údaje by měly být chráněny přiměřenými bezpečnostními zárukami proti rizikům, jako je ztráta nebo neoprávněný přístup, zničení, použití, úprava nebo zveřejnění údajů“ (OECD, 2013, s. 15). Tato zásada pak byla dále přijata v legislativě několika států, včetně Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (známé jako nařízení GDPR). V dubnu 2019 bylo přijato Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií, kterým se zřizuje nový stálý mandát a nový seznam úkolů, přičemž se zdvojnásobují zdroje pro tuto agenturu zodpovědnou za analýzu bezpečnostních incidentů, odborné poradenství, tvorbu doporučení v oblasti kybernetické bezpečnosti, atd. Měla by hrát klíčovou roli při vytváření a udržování rámce certifikace kybernetické bezpečnosti a zvyšování operativní spolupráce na úrovni EU.

Zákon rovněž zavádí celoevropská pravidla pro certifikaci kybernetické bezpečnosti, aby mohly být produkty, procesy a služby certifikovány pouze jednou, zatímco jsou uznávány v celé EU, zejména v oblastech zdraví, energetiky, dopravy a financí. Souběžně se EU rovněž zaměřuje na další průřezová opatření pro řešení kybernetických hrozeb, jako je boj proti organizovanému zločinu, společná zahraniční a bezpečnostní politika a kybernetická obrana (Rada EU, nedatováno). Mezi další stěžejní zákony pak patří Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS) včetně Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) zapracovávající směrnici.

Definicí kybernetické bezpečnosti se ve své publikaci zabýval Dan Craigen se skupinou dalších kolegů analyzováním dostupných definic kybernetické bezpečnosti, integrujících klíčové koncepty čerpané z literatury, kdy dospěl k definici, se kterou je možné i ohledem na provedenou dekonstrukci zcela přijmout. „Kybernetická bezpečnost je organizace a propojení zdrojů, procesů a struktur používaných k ochraně kyberprostoru a zařízení využívajících kyberprostor před událostmi, které se odchylují de jure (podle práva) od de facto (ve skutečnosti) vlastnických práv“ (Craigen, 2014, s. 13). Bezpečnostní incidenty, které jsou v této práci uvažované, lze vnímat jako „incidenty kybernetické bezpečnosti“ a tedy širší množinu událostí, kdy některé z těchto incidentů se po oznámení mění v trestné činy jako „incidenty kyberkriminality“.

3.1.3 Kyberkriminalita

Na jedné straně je potřeba chránit údaje (a zajistit tím jejich bezpečnost), na druhé je jejich shromažďování za účelem následného využití pro trestní řízení. Policie ČR vstupuje do hry většinou poté, co bylo podáno trestní oznámení a dále – kromě informací poskytnutých oznamovatelem, zajišťuje další data z veřejných či soukromých zdrojů. Tedy zpravidla (byť se rovněž věnuje preventivním osvětovým kampaním) vstupuje do procesu až po spáchání trestného činu. V této fázi právě využívá zdrojů původně nastavených pro obecnou obranu budující kybernetickou bezpečnost. Vymezení obou pojmů (a tedy i přijímaných opatření) často splývá, ale přesto dochází k odlišení pojmů „kybernetické

bezpečnosti“ a „kyberkriminality“ (někdy též označované jako kybernetické, informační, elektronické, počítačové, softwarové kriminality atd.). V rámci modelu je pak tato rozdílnost patrná při odlišení „bezpečnostních incidentů“, z nichž některé přecházejí v „oznamovanou trestnou činnost“ a je tedy patrné, že „bezpečnostní incidenty jsou širší množinou prvků než „oznámené trestné činy“, resp. kyberkriminalita.

Jak již bylo zmíněno, existuje zcela nový prostor zahrnující všechny aspekty našich životů, kde lze páchat trestnou činnost. Dle Mezinárodní telekomunikační unie dochází nejen k nárůstu zařízení připojených k internetu, ale především uživatelů internetu – přibližně 53,6 % světové populace – tedy 4,1 miliardy uživatelů a dále tento počet viditelně roste (ITU, nedatováno). Zpráva Accenture tvrdí, že organizace vynakládají čím dál tím vice prostředků na odstranění následků kyberkriminality a vypočítávají celkovou hodnotu rizika na 5,2 bilionu amerických dolarů v následujících pěti letech (Accenture, nedatováno). Také zpráva Europolu o působení organizovaného zločinu ve světě internetu (Internet Organized Crime Threat Assessment – IOCTA) popisuje narůstající počty (i druhy) případů trestné činnosti online, včetně zvyšování počtu kyberkriminality v souvislosti s pandemií Covid-19 (Europol, 2020). Narůstá také obava z osob, které páchají trestnou činnost ze zemí s nedostatečnými zákony (Kshetri, 2005). Odpovědí mezinárodního společenství byla sice Úmluva o kyberkriminalitě z roku 2001, otázkou zůstává, zda země na které je právě toto opatření cíleno, jsou schopni jej dodržovat, například tím, že je u nich vůbec možné řádně dokumentovat všechny incidenty.

Kyberkriminalita je obvykle vnímána v tom smyslu, že informační a komunikační (ICT) technologie jsou buď předmětem útoku, nebo je páchána trestná činnost s jejich podstatným využitím jako prostředku – například při krádeži, vydírání, padělání, mravnostních trestných činech, podvodech, porušení autorských práv, šíření poplašné zprávy, podněcování nenávisti, hanobení národa, rasy, atd. Mohli bychom se setkat i s názory, že jakýkoli trestný čin zahrnující elektronické důkazy je součástí počítačové kriminality, což je zřejmě nesmyslné. Počítačová kriminalita má vliv na již stávající typy kriminality a na druhé straně vytváří zcela nové kategorie kriminality. Existuje však boj o její jasné vymezení a z toho plynoucí statistické vykazování, monitorování a protiopatření. Zatímco ještě před několika lety nebyla kyberkriminalita téměř vnímána a statisticky vyhodnocována, v dnešní době je tak označováno mnoho typů trestných činů. Je obyčejný podvod, jako například nabízení nového mobilního telefonu online bez jakéhokoli úmyslu

jej dodat, stále "podvodem" a nebo bychom jej měli již zařadit pod "kyberkriminalitu", nebo jej problematicky vykazovat v obou skupinách? Česká technická norma říká, že „počítačový zločin je zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený" (ISO/IEC 2382-8, 2001), ale již na první pohled je zřejmé, že norma z roku 2001 neodpovídá nejen technologickému vývoji, ale zaostává i z pohledu trestněprávní terminologie. JUDr. Kolouch (2016) sice ve své publikaci Cybercrime, která zatím v tuzemsku nejšířeji pojednává o problematice kyberkriminality, popisuje obsáhle popisuje problém vymezení kyberkriminality, doporučenou definici však nepředkládá. Pro účely práce – i s ohledem na to, že mezi využitými daty jsou data Policie ČR - je tedy jako kyberkriminalita využita definice Policie ČR, tedy 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 trestná činnost páchána za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání." (Policie ČR, nedatováno/a). Samotné vymezení však není tak zřejmé, aby například v rámci přiřazování atributu „IT kriminalita" v rámci interního systému Policie ČR každý příslušník věděl, co přesně se pod touto definicí rozumí (je například trestný čin porušení autorských práv dle § 270 Trestního zákoníku sdílením audiovizuálních děl přes online uložiště již kyberkriminalita, nebo není?).

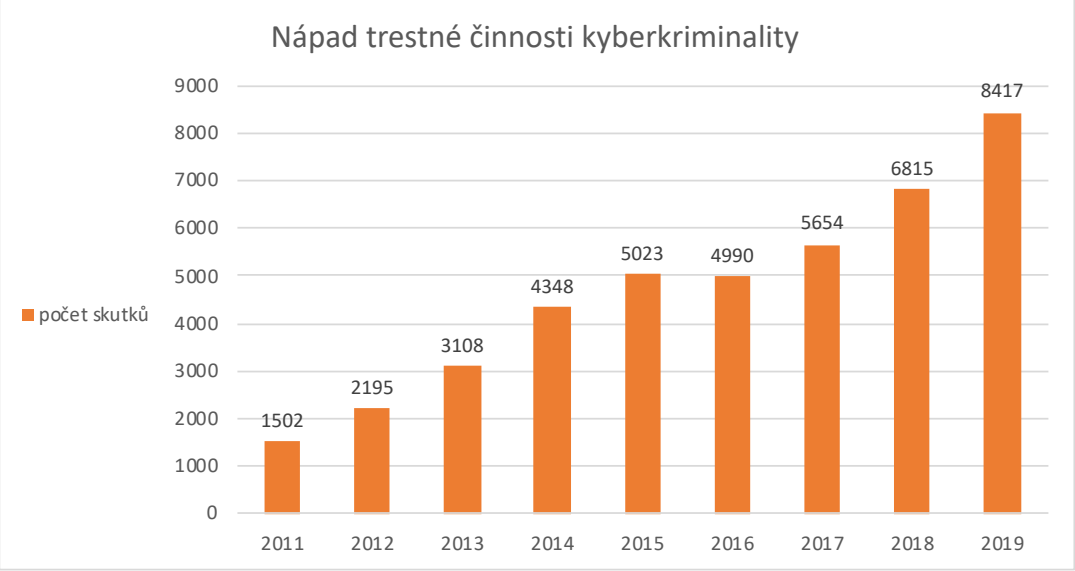
3.1.4 Stav kyberkriminality v ČR

Vedle tzv. ryzích trestných činů kyberkriminality – tedy naplnění skutkových podstat trestných činů uvedených v trestním zákoníku – § 230 - *Neoprávněný přístup k počítačovému systému a nosiči informací* a § 231 - *Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat* se mezi formy kyberkriminality se dnes řadí například kyberterorismus v podobě útoků na funkčnost počítačových systémů a elektronických komunikací (tzv. DDoS útoky, spyware, malware) naplňující skutkové podstaty trestných činů obecného ohrožení, poškození a ohrožení provozu obecně prospěšného zařízení nebo sabotáže, útoky na obsah počítačového systému a předávaných zpráv (vyzvědačství, ohrožení utajované informace) nebo šíření informací (jedná se například o skutkové podstaty trestných činů podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, násilí proti skupině obyvatel a proti jednotlivci, hanobení národa, rasy, etnické nebo jiné skupiny osob, založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka podněcování nebo schvalování trestného

činu). Tyto druhy trestných činů jsou však jen malou částí statisticky vykazované kyberkriminality. Jako nejčastější druh kyberkriminality se totiž uvádí podvody na internetu (podvodné e-shopy, inzeráty, žádosti o půjčky), využívání virtuálních měn při legalizaci výnosů z trestné činnosti, phishingové útoky s cílem získání podvodných přístupových kódů, krádeže identit a odcizení citlivých údajů, ale také již zmíněné porušování autorských práv, neoprávněné držení platebního prostředku, šíření dětské pornografie či využívání anonymity Darkwebu například k nelegálnímu nabízení služeb od průniku do počítačového systému třetích osob a využití sociálního inženýrství za účelem finančního prospěchu pachatelů apod. (Policie ČR, 2019, s. 28 - 31).

Mezi nejznámější typy útoků se pak řadí například botnet (množství kompromitovaných počítačů, pracujících jako tým například v případě tzv. DDoS útoků (omezení dostupnosti služby tím, že je na něj vysláno najednou velké množství požadavků), malware – tedy škodlivý software (trojské koně, viry, různí červi, ransomware blokující přístup k datům a požadování protihodnoty nebo spyware odesílající data bez vědomí uživatele přes internet), či „pharming“ – přesměrování uživatele na podvodný server.

Dle uvedené definice Police ČR a veřejně dostupných statistik pak dochází k nárůstu kyberkriminality a kriminality páchané na internetu, kdy nejpočetnější skupinou jsou různé formy podvodného jednání (více než polovina evidovaných skutků) a pojistné podvody. Počet trestných činů je sledován od roku 2011, kdy dochází k setrvalému nárůstu evidovaných případů kyberkriminality (Policie ČR, nedatováno/a).

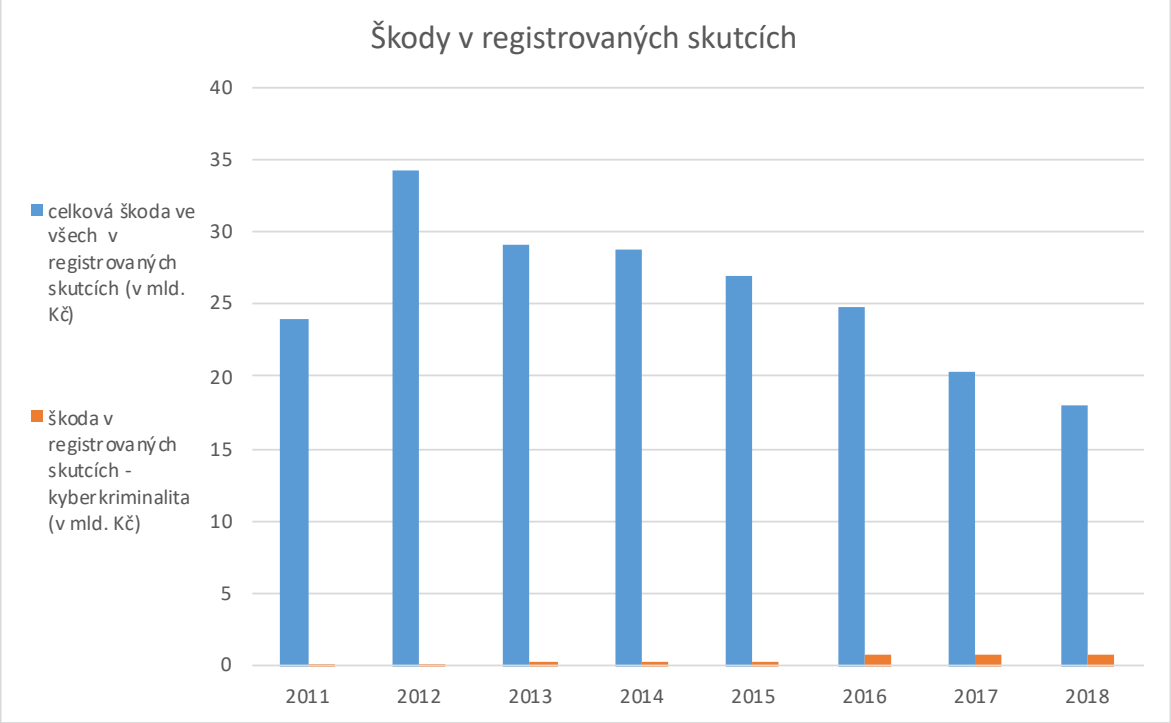


Obrázek č. 1 - Počet registrovaných skutků (nápad) kyberkriminality[3]

Ze statistiky za rok 2019 vyplývá, že „téměř o třetinu vzrostl počet případů tzv. hackingu (na 930), což jsou zejména případy neoprávněného přístupu k počítačovému systému a nosiči informací. Tato skupina trestných činů svým počtem začala převyšovat mravnostní trestné činy. Zajímavý je také vysoký nárůst trestné činnosti spojené s neoprávněným provozováním hazardní hry ve virtuálním prostředí. Významné zastoupení má stále také mravnostní kriminalita (777 skutků), kde znepokojivě roste počet pachatelů do 18 let věku v poměru ke zletilým pachatelům.“ (Policie ČR, nedatováno/a).

Zajímavý je také klesající trend škod v registrovaných skutcích trestné činnosti celkové, avšak zvyšující se počet škod v registrovaných skutcích kyberkriminality.

[3] vlastní zpracování na základě veřejně dostupných dat (Policie ČR, nedatováno/b)



Obrázek č. 2 - Graf škod v registrovaných skutcích[4]

Na rozdíl od škod, které jsou statisticky relativně dobře vykazované, je velice těžké určit náklady spojené s prevencí kyberkriminality. Například v Británii se odhady různí od 27 miliard GBP po 4,1 milionu GBP (Institut pro kriminologii a sociální prevenci, 2019, s. 22). Náklady pak výzkumy dělí na náklady „anticipace“ (technologické, školení, bezpečnostní praktiky, vládní aktivity), „dopadu“ (náklady na řešení útoku, finanční ztráty) a „vynaložené v reakci“ (náklady na vyšetřování a vymáhání práva, soudní řízení, náklady spojené s uvězněním pachatelů, probaci, atd.) (Institut pro kriminologii a sociální prevenci, 2019, s. 36 - 37).

Stejně tak, jako není zřejmá samotná definice kyberkriminality, existuje pouze tenká hranice mezi pojmy kybernetická bezpečnost a kyberkriminalita, kterou lze jen obtížně přesně definovat. Kybernetickou bezpečnost je třeba vnímat jako širší pojetí ochrany, zatímco kyberkriminalita je její součástí, do níž je zapojeno trestní právo, a tedy i jeho vymáhání. Kyberkriminalita je trestná činnost páchaná v prostředí ICT technologií a má dopad na vládní instituce, podniky a občany. Pokud existuje bezpečný kybernetický a veřejný sektor, je obvykle také chráněn před kyberkriminalitou. Zároveň platí, že čím více

[4] vlastní zpracování na základě dat Policie ČR (Policie ČR, nedatováno/b)

bude eliminováno pachatelů kyberkriminality, tím dojde ke zlepšení prostředí z pohledu kybernetické bezpečnosti a ke snížení počtu bezpečnostních incidentů. Strategie pro posílení kybernetické bezpečnosti a pro boj proti kyberkriminalitě se však liší. Je důležité udržet odpovědnost za kybernetickou bezpečnost zejména v rukou soukromého sektoru - implementací mechanismu hlášení, vzděláváním, školením, zálohováním, zabezpečením sítí atd. V boji proti počítačové kriminalitě je pak vhodné zaměřit se na prevenci, adekvátní legislativu, výchovu specializovaných osob orgánů činných v trestním řízení a jejich školení, podporu mezinárodní spolupráce atd.

Základními aktéry kyberkriminality jsou - jako u jakékoliv jiné kriminality - pachatelé a oběti. Do procesu však také vstupují orgány činné v trestním řízení - soud, státní zástupce a policejní orgán (od místních oddělení zpravidla přijímajících trestní oznámení, přes službu kriminální policie a vyšetřování až po specializovanou sekci Národní centrály organizovaného zločinu), pokud provádějí úkony trestního řízení. Mezi další instituce podílející se na procesu prevence a odhalováni kyberkriminality pak patří především Národní úřad pro kybernetickou a informační bezpečnost a sdružení CZ.NIC. K těmto složkám se pak řadí rovněž velké množství dalších soukromých subjektů poskytující služby v oblasti kybernetické bezpečnosti, vzdělávaní apod. Výzkumy uvádí, že spolupráce policie s veřejností má pozitivní kauzální vztah s redukcí trestné činnost a odrazení pachatelů od jejího páchání (Murphy, Cherney, 2001). Orgány činné v trestním řízení a především příslušníci Policie ČR hrající klíčovou roli v přípravném trestním řízení musí spolupracovat se soukromým sektorem tak, aby se vypořádaly s překážkami jako jsou například anonymizace a šifrování a využití a pochopení dalších technologií při získávání důkazního materiálů. Bez těchto nezbytných informací nebudou orgány činné v trestním řízení schopny řádně odhalovat a objasňovat trestnou činnost. Pakliže schopny budou, následná míra odsouzených pachatelů může vést ke snížení míry dalších osob majících v úmyslu páchat trestnou činnost a tedy ke snížení kyberkriminality obecně. Tato spolupráce by neměla být založena pouze na spolupráci pro účely jednotlivých trestních řízení, ale měla by být – i s ohledem na rychle se měnící prostředí - založena na širší spolupráci v rámci sdílení dat a preventivních programů. Osvěta mezi veřejností totiž znamená nižší pravděpodobnost selhání lidského faktoru a tedy možné snížení počtu kybernetických incidentů a kyberkriminality.

3.1.5 Oznamování kyberkriminality

Již při zběžném pohledu na statistické údaje je patrný nepoměr mezi mírou bezpečnostních incidentů a počtu oznámených trestných činů a lze předpokládat, že závisí na několika faktorech, které zpětně ovlivňují počet incidentů. Ze statistik ČSÚ vyplývá, že 20 % obyvatel (24,9 % uživatelů internetu) se v roce 2019 přihodil alespoň jeden bezpečnostní incident na internetu (sledovány byly incidenty typu napadení účtu na e-mailu či sociálních sítích, zneužití platební karty na internetu, krádež totožnosti, zneužití osobních údajů k šikaně, obdržení podvodných e-mailů, přesměrování na falešné stránky, napadení zařízení virem, přístup dětí na nevhodné stránky). Stejné procento – tedy 20 % – uvádí i podniky[5] (dle Statistiky ČSÚ „Informační a komunikační technologie v podnikatelském sektoru ČR, kdy sledovány byly incidenty typu DDoS, ransomware, zničení nebo poškození firemních dat nebo prozrazení důvěrných informací). K tomu je pak pro úplnost nutné zmínit, že přibližně 70 % kyberkriminality zůstává nezjištěno, resp. nedetekováno uživateli (Thomas, 2015) a do statisticky bezpečnostních incidentů se nezapočítává. Dle uvedené statistiky Policie ČR bylo evidováno v roce 2019 celkem 8417 případů kriminality. Vzhledem k tomu, že statistiky uvádějí počet objasněných – který je nižší – lze předpokládat, že se jedná o počet oznámených trestných činů bez ohledu na způsob jejich ukončení (odložení, návrh na podání obžaloby apod.). Ze zřejmého nepoměru pak vyplývá, že naprostá většina incidentů není oznamována. Tento trend lze vysledovat i v zahraničí – FBI uvádí, že pouze 15 % poškozených v roce 2018 oznámilo kybernetický incident (Swinhoe, 2019), výzkum v USA také ukázal, že motivace oznámit trestný čin online je nižší než motivace při oznámení TČ ve fyzickém svět, stejně tak jako důvěra v to, že policie dokáže identifikovat a odstíhat pachatele spíše při spáchání „tradičního“ zločinu, než v případě kyberkriminality (Graham a kol. 2019).

Dle Kaisera je trestní oznámení podávané soukromými fyzickými osobami z velké části podnětem všech trestních stíhání a pouze 2-9 % je vyvoláno vlastní inciativou policie (Kaiser, 1994, s. 238-239). Mezi hlavními poznatky týkajícími se oznamování trestné činnosti (obecně) pak uvádí, že se liší dle věku, sociální vrstvy a typu deliktu a skutečná ochota k podávání trestního oznámení se odlišuje od chování uváděného respondenty v dotazníkovém šetření. Vedle motivů nepodání oznámení jsou důležité i důvody proč je

[5] z 40701 podniků (počet podniků 2019 dle ČSÚ) se tedy jedná o 8140

zahájeno trestní stíhání, jaký je vztah pachatele a oběti atd. Dále uvádí, že mezi nejčastější důvody nepodání trestního oznámení patří přepokládaná neúspěšnost trestního oznámení, nepatrná škoda, hodnocení věci jako soukromé záležitosti, krytí pachatele, časová ztráta nebo potíže s policií. Rozdíl mezi skutečnou a registrovanou kriminalitou označujeme jako latentní (skrytá) kriminalita. Prostřednictvím statistických údajů získáváme informace o skutečné kriminalitě, která je pouze částí kriminality zjevné – tedy té, která vyšla najevo a je evidována v policejní statistice. Přirozená latence se týká té části kriminality, o které se orgány činné v trestním řízení nedozvěděly, umělá latence charakterizuje tu část, o které se orgány činné v trestním řízení dozvěděly, ale nepodařilo se ji objasnit (Gřivna, s. 33).

Jak již bylo uvedeno, kyberkriminalita má určitá specifika, mající vliv na míru oznamování trestné činnosti. Důležitým faktorem je také kvalitní zpracování oznámení a zajištění prvotních důkazů. Ačkoliv samotná informace je nehmotná, zhmotňuje se v prostředí paměťového média a snadno dochází k zániku stop (které jsou pro trestní řízení stěžejní). Vzhledem k nedostatečné osvětě (nejen oznamovatelů, ale také orgánů činných v trestním řízení) tak dochází v prvotní fázi trestního řízení častému zániku důležitých stop, které by mohly sloužit jako důkaz v řízení před soudem. Pakliže je to možné, je od (zpravidla) poškozeného nutné získat data v co nejméně pozměněné podobě (např. originály emailů včetně hlaviček, nosič informací případně alespoň zadokumentovat kopie dat). Některé výzkumy se pak zabývají tím, jaké jsou důvody za tím, že k oznámení kyberkriminality nedochází. Autoři mezi ně řadí problematické vykonávání policejních činností na internetu, nedostatek zdrojů, malý tlak veřejnosti nebo nízkou motivovanost policistů přijímat taková oznámení s tím, že se nejedná o trestnou činnost, kvůli které chtěli sloužit jako policisté (Goodman, 1997. s. 479 - 483). Zajímavý je pak výzkum autorů z The Pennsylvania State University (Bigdoli, Grossklags, 2016), kteří uvádějí, že mezi hlavní problémy neoznámení kyberkriminality patří tyto čtyři:

1. Problém se správnou identifikací kyberkriminality
2. Osvěta k tomu, jakým způsobem hlásit kyberkriminalitu
3. Motivace k oznamování kyberkriminality
4. Rozsah zpětné vazby, která se oznamovatelům vrátí

Dle Policie ČR evidující počty trestných činů v současné době neexistují oficiální odhady míry latentní kriminality a rovněž neexistuje metodika pro provádění výpočtů (či

odhadů) množství a výše škod v souvislosti k latentní kriminalitou (Policie ČR, nedatováno/b).

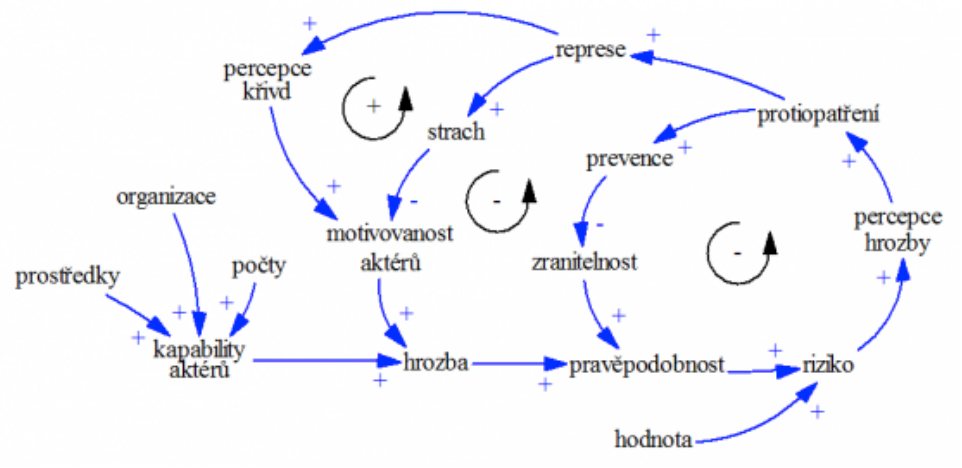
3.2 Systémová dynamika a možnosti její aplikace

3.2.1 Disciplína

K porozumění určitého problému je nutné jej často rozebrat s tím, že jakmile dojde k porozumění jednotlivým částem, snáze pak dojde k porozumění celému celku. Je nutné dohledat vnitřní příčiny, které ovlivňují chování celého systému a řešení problémů, především ta s velkým pákovým efektem - malá změna znamenající velký vliv na chování systému (Šusta, Kostroň, 2004, s. 10). Jak systémová dynamika, tak systémové myšlení využívají tzv. *„mentální model“* kdy vše vnímané je ukládáno do paměti ve formě modelu, který je vytvářen na základě smyslových informací a kombinován s informacemi dosud uloženými v paměti (Šusta, Kostroň, 2004, s. 11). Pokud bude například hovořit občan Ghany s občanem Japonska o vlaku, je předpoklad, že každý bude mít v tu chvíli na mysli jiný obraz v závislosti na své životní zkušenosti. Mentální modely jsou přirozenou součástí lidského myšlení, ale mohou být překážkou pochopení složitějších struktur. Systémové myšlení je však základem pro pochopení systémové dynamiky, která tyto složité struktury umožní chápat lépe.

Pilířem systémové dynamiky je pozitivistický náhled na svět. Jako u přírodních věd je cílem aplikovat numerické metody na komplexní sociální systémy a to především nástroje matematické analýzy a princip zpětné vazby. Pracuje s modely reálných systémů a slouží k simulacím odhalujícím možné dopady lidských rozhodnutí, případně umožní odhalit příčinu skrytých problémů. Mezi známé autory obhajující systémové myšlení patří například Peter Senge, Donella Meadows a především „otec systémové dynamiky“ profesor J. W. Forrester, který se původně zabýval elektroinženýrstvím a vývojem raných počítačových subsystémů a v 60. letech (na Massachusetts Institute of Technology) disciplínu systémové dynamiky založil (Lane, 2007). V České republice se pak přístup rozvíjel již od 70. let, nejprve na vysokých školách a ve výzkumných ústavech, až později si našel cestu do dalších oblastí a především rozvoj IT umožnil aplikaci systémové dynamiky snadno dostupnou širokému spektru uživatelů. Velké užití nachází v řešení business problémů na taktické a strategické úrovni, ale vede k rozvoji chápání komplexních systémů i v jiných oblastech lidských činností a tedy i při rozhodování ve sféře státní správy, kde rovněž umožňuje pochopení struktury a dynamiky měkkých sociálních systémů. Drmola například představuje

a vysvětluje základní principy systémové dynamiky jakožto metodologie či analytického rámce pro výzkum v oblasti bezpečnostních a strategických studií, jako nástroj s jehož pomocí lze zachytit a modelovat konflikty, aktéry, hrozby a bezpečnostní koncepty tak, aby bylo možné vidět nové kauzality a predikovat jejich chování.



Obrázek č. 3 - Příklad ukázky modelu z oblasti bezpečnosti (Drmola, 2014, s. 26)

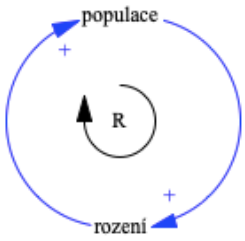
Teorie systémové dynamiky se vždy nejprve věnuje popisu základních teoretických principů systémové dynamiky, kdy základním je uvědomění, že existují určité definovatelné prvky systému, které jsou určitým způsobem propojeny. Dynamika znamená neustálou změnu a tedy vyjádření toho, že se všechny systémy neustále dynamicky mění. Šusta uvádí, že základním principem systémové dynamiky je, že veškeré dynamické chování je důsledkem struktury, kterou se rozumí způsob složení a propojení prvků (Šusta, Kostroň, 2004, s. 16). Nezáleží tedy pouze na jednotlivých prvcích systému, ale rovněž na způsobu, jakým jsou propojeny.

Nejprve byly simulační modely popisovány diferenciálními rovnicemi, zpracovávané kompilátorem SIMPLE (Simulation of Industrial Management Problems with Lots of Equations), později začala být systémová dynamika používána i v jiných oblastech. Již Forrester se zabýval oblastí tzv. „Urban Dynamics“ s cílem zjistit příčiny vzniku míst s vysokou kriminalitou, sociálně vyloučených, apod. S využitím těchto modelů pak demonstroval kontraproduktivnost politik, podle kterých byla města řízena, nepřihlížejících k dynamickému chování sociálních systémů (Forrester, 1995). S čím dál častějším využíváním systémové dynamiky k řešení problémů se rozvíjely i nástroje sloužící k dynamickému modelování – např. Dynamo, Stella, Powersim, Vensim (produkt společnosti Ventana Systems, Inc., použitý k modelování v této práci) umožňující tvorbu

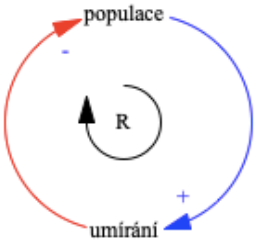
modelů a simulaci dynamického chování systému bez nutnosti znalosti složitých diferenciálních rovnic.

3.2.2 Možnosti popisu struktury systému a základní prvky modelu

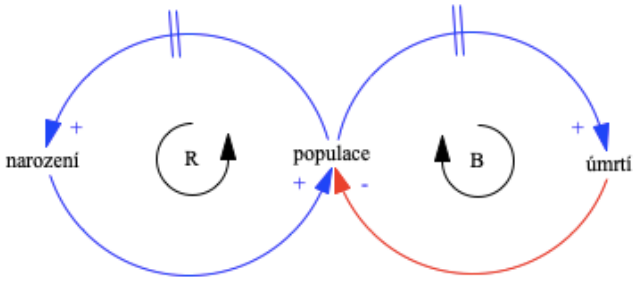
Ke znázornění struktury systému se používají dva základní typy diagramů. Prvním je tzv. příčinně smyčkový diagram (causal loop diagram, CLD) zobrazující zúčastněné entity a vztahy mezi nimi. Druhým pak je tzv. diagram stavu a toků (stock and flow diagram, SFD). Při konstrukci modelu je zpravidla nejprve vytvářen model CLD, resp. diagram kauzálních smyček zobrazující pozitivní (značeny šipkou s „ + “) a negativní vazby (značeny šipkou s „ - “) v modelovaném systému, včetně zobrazení smyček odezvy systému. CLD „zjednodušuje transformace slovního popisu do zpětnovazební struktury, která je uložena v našem mozku v podobě mentálního modelu“ (Mildeová, 2014, s. 290). Diagram představuje jednoduchou mapu systému včetně všech jeho složek a jejich vzájemné interakce. Diagram je snadno pochopitelný i pro laiky (a tedy méně náročný pro tvorbu), ale zobrazuje pouze co by se stalo při změně systému bez více podrobností. Základem jsou zpětnovazební smyčky, které představují přenos a návrat informace. V rámci zpětnovazebních smyček existují pouze dva druhy zpětnovazebních smyček – pozitivní (vychylující systém směrem od rovnováhy) a negativní (působící směrem k rovnováze) a ačkoliv u složitějších systémů může být smyček až tisíce, existují pouze tyto dva druhy. Šusta uvádí, že pozitivní zpětná vazba pak spočívá v přístupu, že čím vyšší/nižší určitá proměnná (a), tím vyšší/nižší další proměnná (b) a čím více/méně (b), tím více/méně (a). Příkladem je pak např. pokud a = populace a b = rození. Negativní vazba spočívá v přístupu, že čím více (a), tím více (b) a čím více (b), tím méně (a). Jedná se například o zpětnovazební smyčku pakliže a = populace a b = umírání (Šusta, 2015, s. 28 – 30).



Obrázek č. 4 - Příklad pozitivní zpětnovazební smyčky[6]



Obrázek č. 5 - Příklad negativní zpětnovazební smyčky[7]



Obrázek č. 6 - Ukázka příčinného smyčkového diagramu[8]

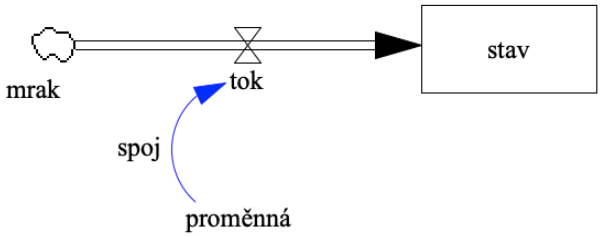
Oproti tomu model SFD je komplikovanější a rozsáhlejší, kdy i jeho tvorba a pochopení zabere více času. SFD diagram je základem pro matematický model (simulační model), který umožňuje podrobnou kvantitativní analýzu. Jak uvádí Sterman, základem je tvorba a výpočet soustavy diferenciálních rovnic, ale k pochopení stavů a toků, které jsou používány pro zachycení zpětnovazební struktury systému, není hlubší matematická znalost podmínkou. Model dokáže znázornit odlišit stavy a toky a umožní provádět simulace, kde prostor a čas je komprimován a umožní tak vidět dlouhodobý (a někdy i vedlejší) účinky rozhodovacího procesu (Sterman, 2000). SFD tak umožní vyhnout se některým interpretačním problémům, vznikajícím u příčinných smyčkových diagramů. CLD slouží k zobrazení vyšší úrovně k pochopení celého systému, zatímco SFD se zaměřuje na podrobnou analýzu určité části zkoumaného systému. V rámci modelu SFD jsou vztahy CLD převedené do detailnějšího popisu skrz parametry jednotlivých objektů modelu.

[6] vlastní zpracování

[7] vlastní zpracování

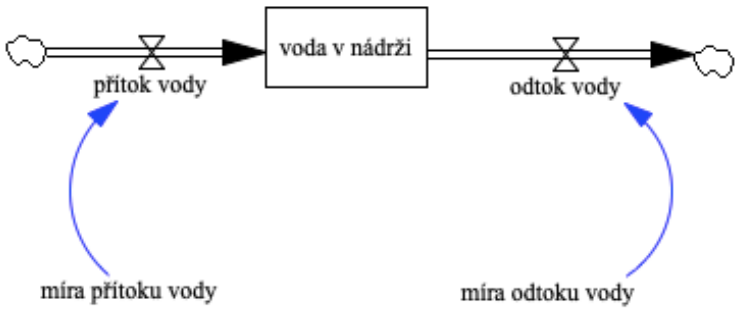
[8] vlastní zpracování

Složky systému lze rozlišit na veličiny endogenní (uvnitř systému), které se mohou měnit v průběhu času a exogenní (vně systému, které ale systém ovlivňují) a mohou se měnit v čase a rovněž veličiny, které se v době sledovaného vývoje nemění. Základními veličinami jsou tzv. *stavové proměnné* – což jsou proměnné akumulující změny v této práci znázorňované obdélníkem (jedná se o entitu, která se časem hromadí a spotřebovává) a *toky* které tyto stavy ovlivňují (specifikují jakou mírou daná entita přibývá nebo ubývá) označené jako dvojitá šipka. Autoři, zabývající se systémovou dynamikou, často připodobňují tyto proměnné k rezervoáru kapaliny (stav). Tyto mají přítok, resp. tok (vyjadřující kladnou část dynamické rovnice) a odtok, resp. tok (vyjadřující zápornou část dynamickou rovnice), které regulují změnu stavové proměnné. Dalšími částmi modelu jsou tzv. *pomocné proměnné* – pomocné informace nebo konstanty. Do celkové koncepce modelu patří také tzv. *mraky* znázorňující hranice modelu a *spoje* propojující různé prvky modelu a tedy tvořící vazby mezi stavy, proměnnými a toky (Šusta, 2015 a Mildeová, Vojtko, 2008).



Obrázek č. 7 - Stavební bloky modelu[9]

Proměnné lze aplikovat na konkrétní příklad následujícím způsobem.



Obrázek č. 8 - Ukázka stavebních prvků na praktickém příkladu[10]

[9] vlastní zpracování

[10] vlastní zpracování

Tento model (na obr. č. 9) pak říká, že odněkud (co už je za hranicemi námi modelovaného systému – může se tedy jednat o kohoutek, množství srážek apod.) přitéká voda „přítokem vody“, která ovlivňuje množství vody v nádrži. Tato pak odtéká pryč „odtokem vody“ (hadicí, kohoutkem, dírou ve dně nádrže apod.) opět za hranice zkoumaného modelu. Přítok i odtok vody jsou pak ovlivněné mírami přítoku/odtoku vody. Do modelu je pak možné zaznamenat i další proměnné (informace, konstanty), které ovlivňují tyto míry (např. úhrn srážek, otevřený/zavřený dílčí odtokový nebo přítokový kanál, míru zanesení koryta přítoku apod.).

Mezi typické způsoby chování systému patří:

- Lineární vývoj – stabilní růst/pokles, kdy ke změně dochází konstantní rychlostí, resp. není zde žádná zpětná vazba.
- Exponenciální růst – rychlost změn je úměrná velikosti zásobárny, kdy systém je řízen pozitivní vazbou
- Logistický vývoj – kombinace pozitivní a negativní vazby, v první fázi dochází k exponenciálnímu růstu, avšak poté je následován přibližováním s rovnováze
- další (např. přestřel a kolaps nebo oscilace)

Některé struktury se stále vracejí – tzv. systémové archetypy. Jedná se o určité struktury, které jsou klíčem k pochopení struktur složitějších systémů. Vyjadřují jednoduchost, která se skrývá za komplexností problémů. S ohledem na rozsah práce není nutné jednotlivé archetypy detailněji popisovat, pro celkový úhel pohledu je však nutné je alespoň zmínit. Mezi ty nejznámější patří například „Meze růstu“, „Tragédie společného“, „Úspěch úspěšným“, „Eskalace“, „Eroze cílů“ a další (Šusta, 2015).

3.2.3 Aplikace systémové dynamiky

Dle autorů Vojtka a Mildeové (2007, s. 88 – 89) lze proces aplikace systémové dynamiky rozdělit do několika fází. V té první je nutné definovat účel, který umožňuje posoudit co je a není podstatné. Tím dojde i definici hranic zkoumaného systému a pochopení podstaty problému. V další části pak dochází k objasnění chování systému jako celku, který je zodpovědný za zkoumaný problém, k čemuž mohou být využity nástroje jako diagram hranic systému, diagramy subsystému a CLD a SFD diagramy (použité v této bakalářské práci). Formulací simulačního modelu se pak rozumí sestavení simulačního modelu, který je nutný k odvození logických důsledků. Za tímto účelem je nutné většinu zadaných vlastností kvantifikovat, případně doplnit matematické vztahy mezi prvky modelu.

Poslední částí je pak testování modelu, tedy vytvoření dynamické hypotézy o příčinách chování systému.

Simulační model lze pak využít pro účely zhodnocení (zjištění, zda předpokládané změny vyhovují požadavkům), k porovnání (porovnání efektů při různých nastavení pravidel), citlivostní analýze (identifikaci faktorů, které zásadní měrou ovlivňují zkoumaný systém) případně k optimalizaci (určení takového nastavení hodnot faktorů, vedoucích k požadované hodnotě zvoleného kritéria). Jak uvádí Šusta „Když chování pochopíte, můžete experimentovat se změnami ve struktuře. Tím vyvoláte žádoucí chování. Když model (přiměřeně) vyjadřuje opravdový problém, můžete ho používat pro analýzu a experimentování. Máte potom jakousi mini laboratoř, ve které můžete simulovat důsledky rozmanitých změn politiky před tím, než je zavedete do praxe – do reálného systému“ (Šusta, Kostroň, 2004, s. 36).

Přístup systémové dynamiky byl například použit v případě simulace systému trestního soudnictví v New Yorku, kde zkoumal vliv změny exogenních proměnných - zdvojnásobení počtu delikventů a zdvojnásobení produktivity policie (Macdonald, Mojtahedzadeh, 2014), rozdíl mezi vlivem proaktivního a reaktivního přístupu investic do systému řízení bezpečnosti informací - konkrétně v petrochemickém průmyslu (Qian, 2012) nebo v případě zkoumání schopnosti policie řešit kriminalitu s využitím spolupráce s veřejností, kdy metodou systémové dynamiky prokazoval, že kooperativní vztah s veřejností může být strategickým nástrojem efektivní kontroly kriminality bez nutnosti zvyšování výdajů na činnost policie (Lee, Jung, 2017). Zajímavý přístup k využití systémové dynamiky je pak v závěrečné práci Lezanie Coetzee (2015), který je především kvalitní a detailní aplikací metody systémové dynamiky na problém drogové kriminality, jenž její vývoj přirovnává k šíření nakažlivé nemoci. Simulace dle metod systémové dynamiky pak autoři také využili k modelování cyklů gangů a jejich kriminálně závadového jednání, kdy na základě simulace dokazují, že jakýkoliv přístup k válce s gangy musí adresovat rovněž sociální a ekonomické aspekty problému (Skarin a kol. 2009).

4 Vlastní řešení

4.1 Dostupná data

Modely, které jsou v rámci této práce vytvořeny by bylo vhodné dále upřesňovat osobami k jejichž rozhodovacímu procesu by mohly prospět, na základě jim dostupných interních dat. V tuto chvíli je však vycházeno z veřejně dostupných dat – především Policie ČR (týkající se počtu oznámených trestných činů, počtu objasněných skutků, škod způsobených trestnou činností, atd.). V těchto lze pak spatřovat největší riziko, co se výpovědní hodnoty týče. Jak již bylo naznačeno v teoretické části práce, definice kyberkriminality stále není zřejmá a tak záleží na tom, kdo statistické údaje v rámci Policie ČR vykazuje a jak široce definici kyberkriminality vnímá (např. trestný čin podvodu může být vykázán v rámci obecné trestné činnosti a pokud v určité míře dojde k použití výpočetní techniky, může být již zařazen do kyberkriminality), ačkoliv je snaha spojovat prověřování trestné činnosti do společných řízení, často k tomu není dostatek informací a tak jsou oznámení vedena pod více čísly jednacími jako více trestných činů, apod. V neposlední řadě jsou vykazované hodnoty zatíženy vysokou mírou latence. Nicméně pro účely této práce však lze konstatovat, že statistiky vykazované Policií ČR jsou dostatečné. Dalším důležitým zdrojem dat je pak Český statistický úřad, jehož data lze (s ohledem na robustnost výzkumných metodik) považovat za velmi vypovídající. Z těchto dat jsou čerpána data o počtu obyvatel ČR a počtu uživatelů internetu (statistika „Počítač a internet v českých domácnostech“). Bohužel údaj o počtu bezpečnostních incidentů, resp. počtu jednotlivců, kterým se v posledním roce přihodil alespoň jeden bezpečnostní incident na internetu (Statistika „Bezpečnost ICT“) je až nově měřenou statistickou proměnnou a tak bylo nutné dopočítat údaje za předchozí roky.

4.2 Tvorba CLD modelu

Šusta a Kostroň (2004, s. 16) uvádí, že důležitým faktorem při tvorbě modelu je modelovat *problémy* nikoliv *systémy.* Ačkoliv tedy tvorba modelu může svádět k tomu začlenit do něj všechny možné proměnné, je důležité soustředit se pouze na proměnné ovlivňující zvolený problém, kterým byl zvolen problém kyberkriminality v ČR. Definování problému znamená zpravidla i definování samotného účelu modelu, který směřuje k pochopení problému. Především je důležité vymezit hranice a vynechat vše, co nesouvisí s chováním problému, který je zkoumán. Smyslem modelu je postihnout pouze tu část reality a zahrnout právě tolik prvků, které jsou nezbytné k vyjádření chování problému. Je však

důležité nenechat řešení spadnout do tzv. „špagetového diagramu“, byť je to za cenu zjednodušení popisu problému. Modelování problému je vždy jen určitou reprezentací reality a „pro každý komplexní problém je řešení, které je jednoduché, přesné a špatné“ (Love, 2009). V první fázi byl vytvořen obecný příčinně smyčkový diagram, který zobrazuje vztahy mezi entitami. Dochází k analyzování problémové situace ve které je uvažována případná změna. V této části dochází k identifikování veškerých relevantních částí systému, které budou mít vliv na řešenou část a zároveň je v rámci této fáze bezpodmínečně nutné stanovit hranice systému, aby model nebyl příliš komplexní. Byly tedy stanoveny proměnné, ovlivňující kyberkriminalitu v ČR a následně identifikovány vazby mezi těmito proměnnými. Na základě modelu pak byly vyhledány body, v rámci kterých je možné na systém působit a stanovit nejvhodnější místo k působení. Tyto proměnné pak jsou dále využity v rámci SFD diagramu. V některých případech jsou proměnné zobecněny – jako například v případě motivace, jež je vyjádřena jednou proměnnou, ačkoliv se skládá z několika dalších proměnných, které by bylo vhodné pro účely zkoumání též zakomponovat do modelu a kvantifikovat. Do modelu by bylo možné též zakomponovat další smyčky – například společenské vlivy, dobu, po kterou trvá pachatelům najít jejich zranitelnosti, na které je reagováno jejich zacelením a protiopatřením, což vytváří v modelu systémové dynamiky smyčku, ale to by již vedlo k jeho zbytečné robustnosti.

Důležité bylo postupné přidávání smyček – částí celkového diagramu, ty stěžejní pak byly identifikovány tímto způsobem:

Identifikované zásadní smyčky CLD modelu:

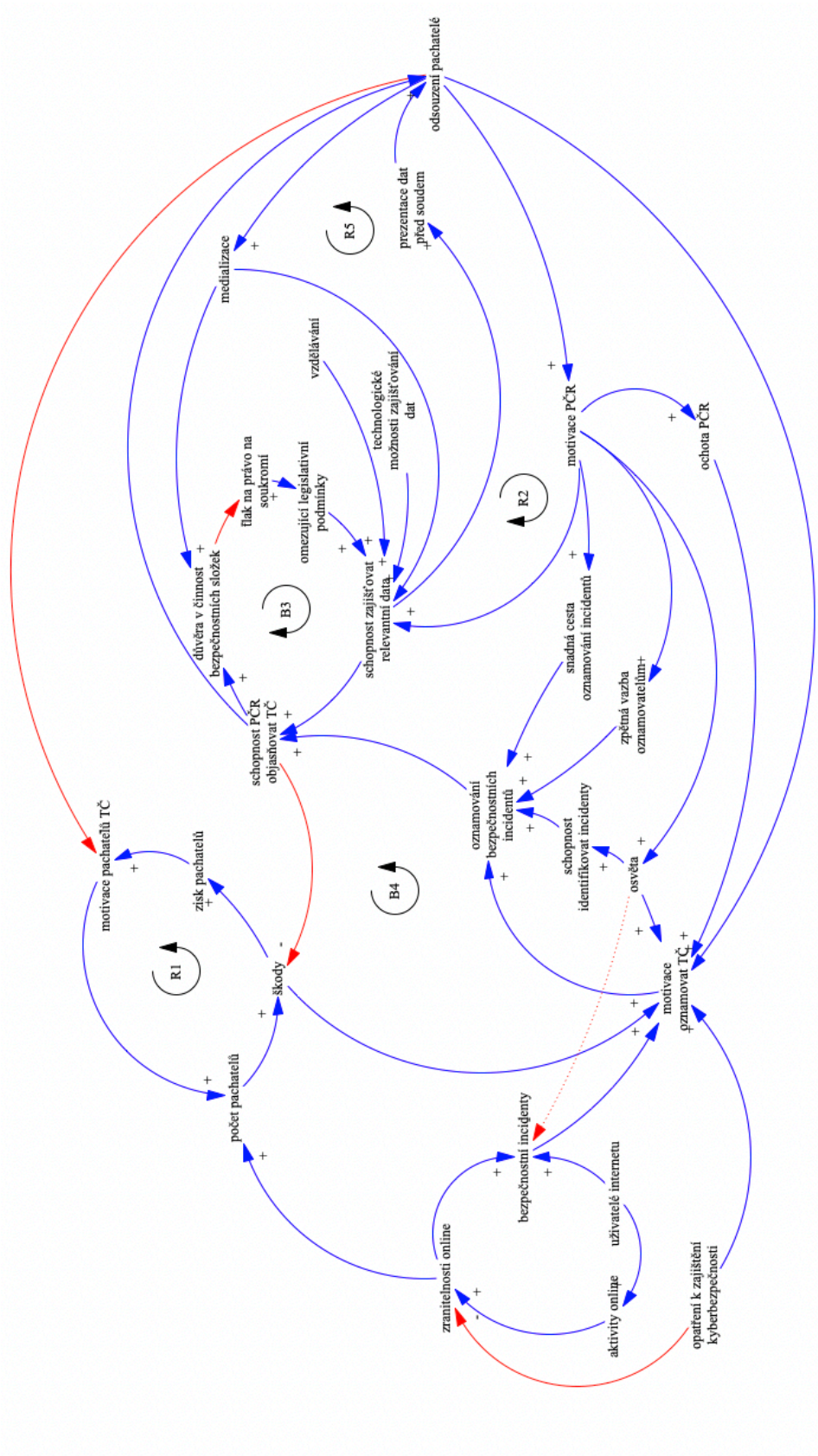
- R1 – Sebeposilující smyčka **„Počet pachatelů“** – Vzrůstající počet zranitelností online má vliv na vzrůstající počet pachatelů, tzv. „příležitost dělá zloděje“. Tito pachatelé jsou především motivováni ziskem (i pokud se jedná o průnik dat do systému, odcizení databáze, zpravidla to je za účelem dalšího zpeněžení získaných dat), čím větší jsou poškozeným způsobené škody, tím narůstá zisk pachatelů, čímž narůstá jejich motivace k dalšímu páchání trestné činnosti. Ve vztahu však vystupuje omezující podmínka – odsouzených pachatelů, kdy tato část diagramu připomíná archetyp systémové dynamiky „meze růstu“, tedy počet pachatelů je omezen určitou mezí, tedy tím, jak je systém schopen tyto pachatele odhalovat a soudit.
- R2 – Sebeposilující smyčka **„Schopnost PČR zajišťovat data“** – Pro kvalitní výstupy Policie ČR je nutné, aby byla schopna zajišťovat relevantní data. Tedy ta, která

mohou sloužit jako důkaz před soudem a na jejichž základě je možné pachatele odsoudit. V rámci trestního řízení totiž může s ohledem na charakter digitálních stop, jenž bývají v procesu často stěžejními, dojít k jejich zániku, případně poškození. Shromážděná data nemusí být vždy považována za přípustné důkazy. Například pokud byly získány na základě nezákonných zásahů do práv a svobod, nelze je v trestním řízení využít. Ačkoliv v českém právním řádu neexistuje generální klauzule stanovující podmínky vyloučení důkazu, dochází k případům, kdy k důkazům není v řízení přihlédnuto a pachatel není odsouzen. Jakmile jsou zajištěna relevantní data, dalším krokem je jejich řádná prezentace před soudem, která by měla vést k odsouzení pachatele. Čím více je pak pachatelů odsouzeno, tím více jsou příslušníci Policie ČR motivováni k práci na dalších případech. To často znamená sebevzdělávání nejen v IT oblasti, ale i trestněprávní a je zřejmé, že čím více jsou motivováni, tím se zpětně zvyšuje jejich (a tedy celé PČR) schopnost zajišťovat relevantní data.

- B3 – Vyvažující smyčka – **„Rovnováha mezi zájmem veřejnosti na odhalení pachatele a zájmem na ochraně soukromí“** – Trestní právo respektuje demokratické a humanitární hodnoty, jako jsou život, zdraví a lidská důstojnost obětí i pachatelů. Ačkoliv jsou lidská práva vnímána jako obecná a nedotknutelná hodnota, prakticky v celém procesu dokazování existuje potřeba tato práva porušovat (zajištění věcí a osob, narušení soukromí apod.) a zpravidla jsou tyto zásahy negativně vnímány. Smyčka pak znázorňuje vztah, kdy jakmile jsou nastaveny příliš omezující legislativní podmínky, znemožňuje to schopnost zajišťovat relevantní data. Čím více je schopnost data zajišťovat, tím větší je schopnost Policie ČR objasňovat trestnou činnost. Čím větší je objasněnost, tím větší je důvěra v činnost bezpečnostních složek. Čím méně důvěry v jejich činnost, tím větší bude veřejnost vyvíjet tlak na právo na soukromí. Pro výpočet systémově dynamického modelu proměnné svobody je pak možné využít výpočet pro proměnnou dle Saeeda a Pavlova znázorňující potlačení lidských práv a vzniku „státem kontrolované“ společnosti na jedné straně a větší sociální svobody na straně druhé (Khalid, Pavlov, 2006). Důvěra v činnost policie vzrůstá (výsledky agentury STEM uvádějí, že v roce 2011 byla 54 % a do roku 2019 vzrostla na 72 %), ale pravomoci Policie ČR jsou stále diskutovány (například diskuze a soudní řízení o uchovávání provozních a lokalizačních údajů). Značné vychýlení však není žádoucí ani na jednu stranu.
- B4 – Vyvažující smyčka – **„Motivace oznamovat incidenty na základě způsobené škody“** – Čím větší je uživateli způsobena škoda, tím větší má motivaci bezpečnostní

incident oznámit. Čím větší je tato motivace, tím spíše bezpečnostní incident oznámí. Spolupráce s veřejností znamená i to, že uživatelé vědí, jaké incidenty oznamovat a jakým způsobem a jaká data Polici ČR poskytnout. Čím větší množství informací má Policie ČR k dispozici, tím spíše je může využít v rámci trestního řízení, čímž se zvyšuje její schopnost objasňovat trestnou činnost. Je možné, že v rámci jednoho oznámení je možné zjistit IP adresu připojení pachatele, v rámci jiného jeho email, kdy lze následně (a pouze kombinací informací z různých spisových materiálů) propojit virtuální osobnost s reálnou. Pakliže by byla řízení vedena odděleně, vedla by pouze k odložení všech, avšak jejich kombinace a propojení všech informací by umožnila trestnou činnost dokázat a s návrhem na podání obžaloby předat státnímu zastupitelství k úspěšnému dokončení trestního řízení. Zpětnovazební smyčka je pak uzavřena tím, že schopnost objasňovat trestnou činnost má vliv na redukci výše škody a tedy opět na motivaci oznamovat incidenty.

- R5 – **„Medializace případů“** – Velice důležitý aspekt celého procesu je zpětnovazební smyčka znázorňující vztah činnosti Policie ČR a medializace. Čím více bude mít Policie ČR informací, tím lépe může připravit trestní spis k jeho prezentaci před soudem. Čím lepší pak tato prezentace je, tím spíše dojde k odsouzení pachatele. Dobrá práce Policie ČR se pak snadno prezentuje v médiích, kdy tato medializace znamená lepší předávání informací a zpětně schopnost zajišťovat relevantní data.



Obrázek č. 9 - Příčinný smyčkový diagram kyberkriminality – znázornění hlavních zpětných vazeb

4.3 Tvorba SFD modelu

Další fází při aplikaci systémové dynamiky ke zkoumání zvoleného problému byla tvorba SFD modelu. Na základě zpracování CLD modelu byly zvoleny části, na které by bylo vhodné v rámci modelu působit za účelem snížení přírůstku kyberkriminality v ČR. Tyto pak byly převedeny do formy proměnných v diagramu. Důležitou jednotkou, která je v procesu znázorněna jsou „incidenty“, které se v průběhu procesu přeměňují na „trestné činy“ jejich oznámením. Ačkoliv o tom, co je a není trestným činem, rozhoduje řízení před soudem, lze pro účely modelu uvažovat, že trestným činem je jakékoliv oznámení, které je Policií ČR takto evidováno.

Cílovými stavy, ke kterým proces směřuje (tedy hodnoty, kterých může incident v rámci celého procesu dosáhnout), byly zvoleny „Počet oznámených trestných činů“ „Latentní kriminalita“ (tedy neoznámené trestné činy) a „Celková škoda“. Nejprve byly určeny jednotlivé prvky diagramu stavů a toků. Jako hranice modelu (mraky) byly zvoleny: počet obyvatel ČR, ze kterých se někteří mění v uživatele internetu a dále incidenty, škody a oznamování, ze kterých dále „čerpají“ toky zvyšování úrovně oznamování, přibývání uživatelů, počtu incidentů a škody. Následně byly v rámci modelu určeny parametry modelu – tedy vzorce a hodnoty. Některé z proměnných lze na podkladě dostupných dat vyhodnotit relativně přesně, další data (tzv. „soft“ proměnné) jsou více neuchopitelné a hůře vyčíslitelné, byť jejich vliv na systém může být stěžejní. Koeficienty se projevují až od roku 2020, kdy nejsou k dispozici reálná data – tedy model do roku 2019 reflektuje stav dle reálných dat. V programu Vensim byla ke zpřesnění hodnot provedena parametrizace – tzv. „payoff funkcí“ využívající modifikovaný Powellův algoritmus (Ventana Systems, 2010, s. 247-254).

Počáteční stav se uvádí vždy jen u stavových proměnných. U toků a proměnných není a tedy při zadávání hodnot (na rozdíl při zadávání hodnot u stavů) při práci v programu Vensim se ani nezobrazuje nabídka vyplnění pole „Intitial Value“. Do pole „Equations“ se pak vkládají rovnice, kdy proměnné se vkládají ze sekce „Variables“, zobrazují se (a je možné tedy použít do rovnice) jen názvy objektů, které mají vazbu na zvolený objekt. Pakliže je v rovnici použito slovo INTEG, znamená, že objekt je „stav“. Například „počet uživatelů online = INTEG (přírůstek počtu uživatelů, 1234)“ vyjadřuje, že se jde o stav s rovnicí přibývání počtu uživatelů online s počáteční hodnotou 1234, případně může být počáteční hodnota vyčíslena jako další proměnná).

Nastavení modelu: Initial time = počáteční čas = 2011, Final time = čas, kdy se model zastaví = 2030, Units for Time: význam „1“ – v případě tohoto modelu byl zvolen „ROK“, Integration time: Euler.

Stavební bloky SFD vyjadřující hodnoty jednotlivých proměnných

Stavové proměnné

- (U) Počet uživatelů: Počet uživatelů = INTEG (přibývání uživatelů, počáteční množství uživatelů)
- (I) Počet bezpečnostních incidentů: Počet bezpečnostních incidentů = INTEG (přibývání počtu bezpečnostních incidentů-oznamování trestné činnosti-vznik latentní kriminality, počáteční množství bezpečnostních incidentů)
- (O) Počet oznámených TČ: Počet oznámených TČ = INTEG (oznamování trestné činnosti, 1502), dále by bylo možné přidat do modelu toky rozdělující počet na objasněné a neobjasněné, ale vzhledem k tomu, že průměrná objasněnost je od roku 2011 cca. 50 % nebyl již model tímto způsobem rozšířen. V rámci statistického vykazování je možné (a velice pravděpodobné), že v roce oznámení nedojde ke sdělení obvinění pachateli (tedy k objasnění trestného činu), ale dojde k němu až v následujících letech. Z pohledu modelu lze však předpokládat, že v určitém roce dojde k objasnění starších oznámení, kdo toto zpoždění není pro účely modelu relevantní a je tedy zanedbáno.
- (L) Latentní kriminalita: Latentní kriminalita = INTEG (vznik latentní kriminality, 1698200), v této stavové proměnné dochází ke kumulaci neoznámených bezpečnostních incidentů. Často dochází k tomu, že je uživatel poškozeným a dlouhou dobu o tomto ani neví, kdy může přijít oznámit trestný čin i zpětně. Zároveň v rámci modelu vzniká určitá „zásobárna“ incidentů, ze kterých je možné z pohledu Policie ČR kdykoliv v budoucnu čerpat, proto se i z tohoto důvodu incidenty v tomto stavu kumulují.
- (Š) Celková škoda: Celková škoda = INTEG (aktuální škoda, 0)
- (M) Míra oznamování: Míra oznamování = INTEG (zvyšování úrovně oznamování, počáteční míra oznamování)

Tokové proměnné (vztahy vyjadřující vždy jednotku za určitý čas)

- Rate_1: přibývání počtu uživatelů = dU/dt = podíl nárůstu uživatelů*Rozdíl mezi max a aktuálním počtem uživatelů
- Rate_2: přibývání počtu bezpečnostních incidentů = dI/dt = míra přibývání počtu bezp. incidentů*Počet uživatelů
- Rate_3: oznamování trestné činnosti = dO/dt = IF THEN ELSE(Time<2020,(přibývání počtu bezpečnostních incidentů*Míra oznamování/100),(přibývání počtu bezpečnostních incidentů*Míra oznamování/100)*změna oznamování bezpečnostních incidentů)
- Rate_4: vznik latentní kriminality = dL/dt = přibývání počtu bezpečnostních incidentů-oznamování trestné činnosti

- Rate_5: aktuální škoda = dŠ/dt = průměrná škoda na skutek*přibývání počtu bezpečnostních incidentů
- Rate_6: zvyšování úrovně oznamování = dM/dt = podíl nárůstu oznamování*Rozdíl mezi max a aktuální mírou oznamování

Další proměnné

- Podíl nárůstu uživatelů = 0.100656
- Rozdíl mezi max a aktuálním počtem uživatelů = Maximální počet uživatelů-Počet uživatelů
- Maximální počet uživatelů = 9963180[11]
- Míra přibývání počtu bezp. incidentů koeficient = 0.249
- Míra přibývání počtu bezp. incidentů = IF THEN ELSE(Time<2020, "míra přibývání počtu bezp. incidentů koeficient", "míra přibývání počtu bezp. incidentů koeficient"*změna přírůstku počtu bezpečnostních incidentů)
- Průměrná škoda na skutek = 99104
- Podíl nárůstu oznamování = 0.293753
- Rozdíl mezi max a aktuální mírou oznamování = Maximální míra oznamování-Míra oznamování
- Maximální míra oznamování = 0.394065

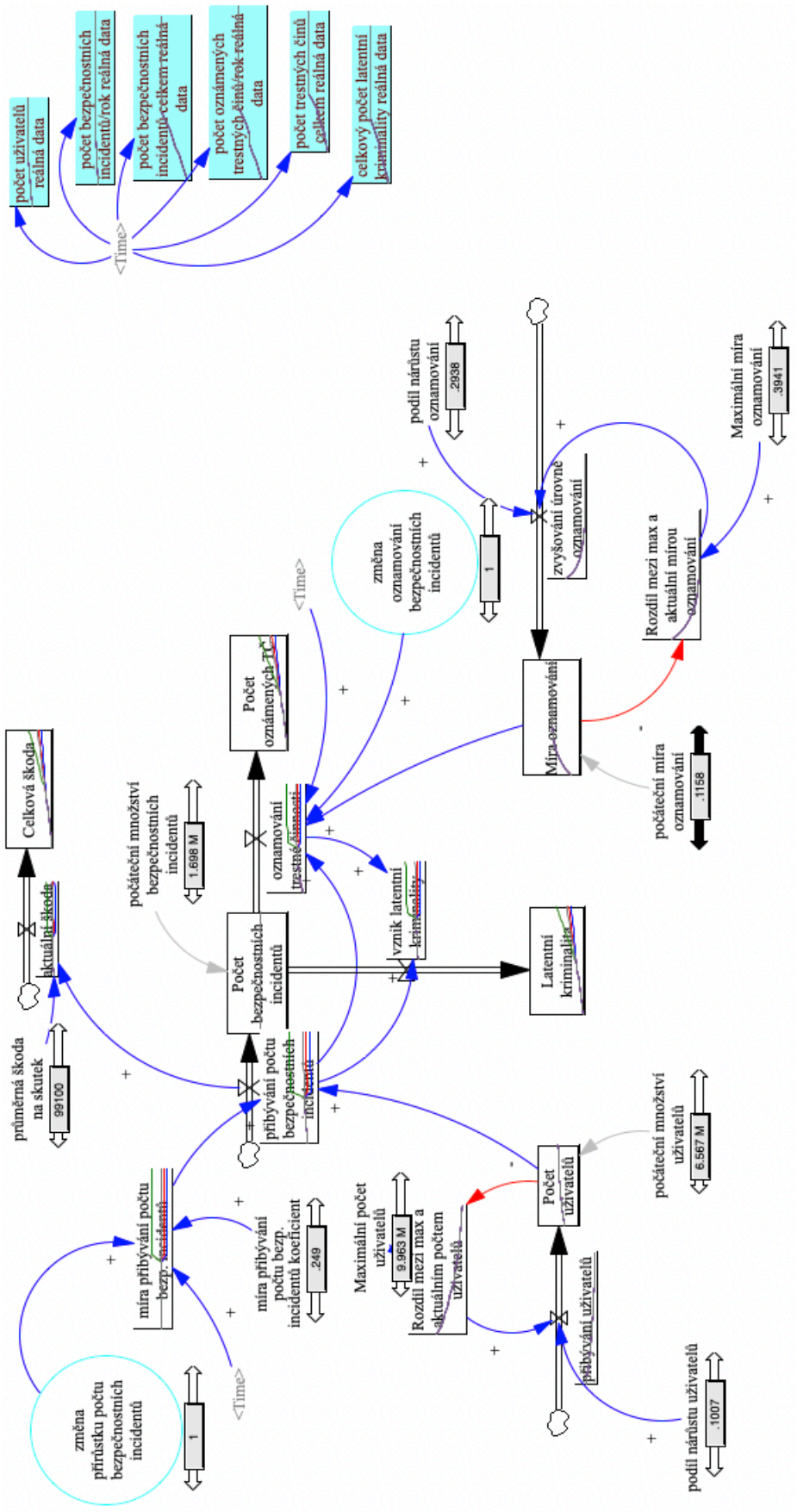
Zkoumané proměnné (konstanty)

- **Změna přírůstku počtu bezpečnostních incidentů** = 1 – koeficient umožňuje při simulaci regulovat další proměnné (v tomto případě „míru přibývání bezp. incidentů“). Při výchozí hodnotě 1 má tedy pouze průměrný vliv na základě historických dat.
- **Změna oznamování bezpečnostních incidentů** = 1 – koeficient umožňuje při simulaci regulovat další proměnné (v tomto případě „oznamování trestné činnosti“). Při výchozí hodnotě 1 má tedy pouze průměrný vliv na základě historických dat.

Počáteční hodnoty – počáteční množství uživatelů (6566950), počáteční míra oznamování (0.115765), počáteční množství bezpečnostních incidentů (1698200)

Reálná data – počet uživatelů reálná data, počet bezpečnostních incidentů/rok reálná data, počet bezpečnostních incidentů celkem reálná data, počet oznámených trestných činů/rok reálná data, počet trestných činů celkem reálná data, celkový počet latentní kriminality reálná data – byla do modelu přidána cestou **„Auxiliary - with Lookup - As Graph“**, tedy postupně byly zadány konkrétní hodnoty za roky 2011-2019 dle „Zdrojových dat“ (uvedené v příloze bakalářské práce).

[11] číslo nalezeno dle Powellova algoritmu, viz. vysvětlení výše



Obrázek č. 10 - Model SFD se základním nastavením proměnných v náhledu SyntheSim

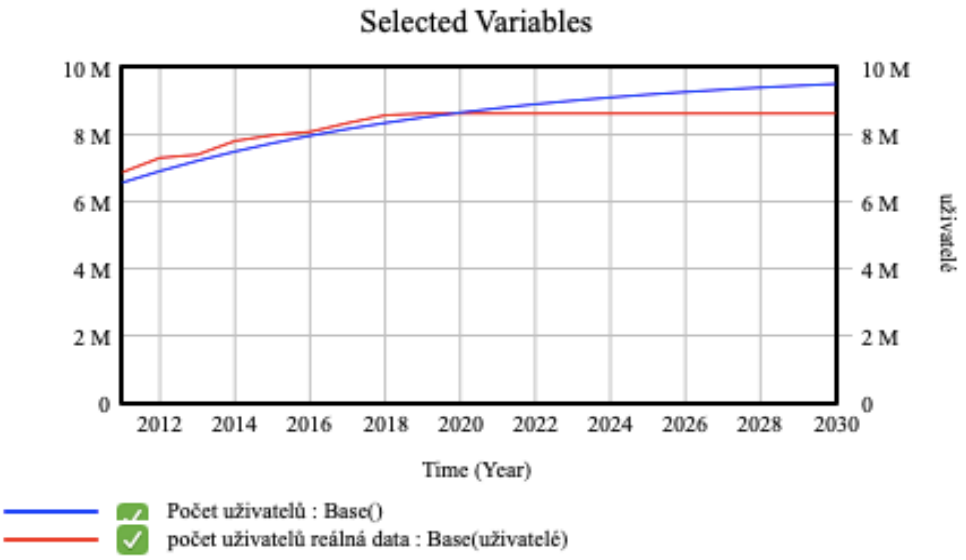
4.4 Testovací simulace SFD modelu pro období 2011 až 2019

Každý model musí být důkladně otestován. Testovací běh modelu simuluje období od roku 2011 do roku 2019, ke kterému existují dostupná data k porovnání. Závislost reálných dat k simulovaným je možné znázornit graficky přímo v programu Vensim (viz. obrázky v této kapitole), kdy je zřejmé, že reálná data odpovídají datům simulovaným. Ke kontrole byl však rovněž využit výpočet dle MAPE – tedy průměrné procentuální chyby odhadu, který měří přesnost predikce odhadu. Vyjadřuje se jako poměr definovaný vzorcem (Khair a kol. 2017, s. 14), kdy y1 je skutečná hodnota a yt je hodnota předpokládaná:

$$MAPE = \frac{\sum \frac{|y1 - yt'|}{y1}}{n} * 100\%$$

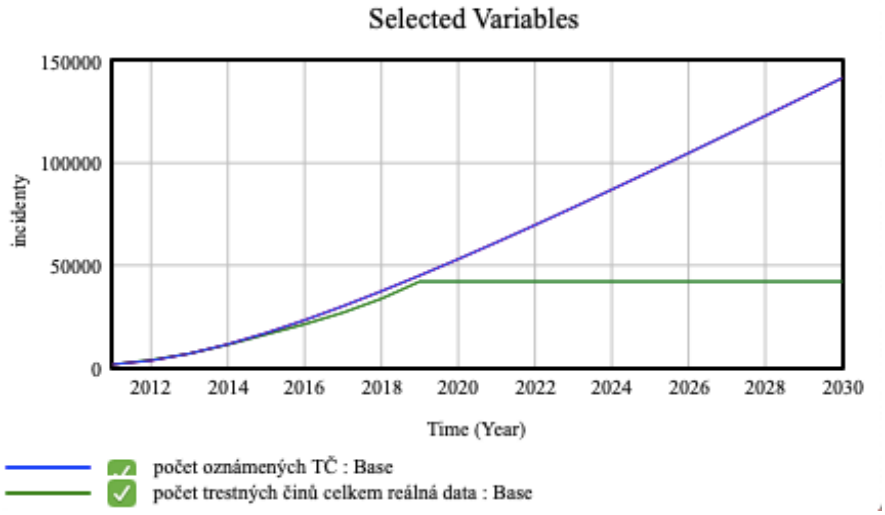
Výsledky této metody jsou zpravidla vyhodnoceny jako výborné, pakliže jsou pod 10% hranicí (Gilliland, 2010). Při srovnání reálných dat a dat simulovaných v letech 2011 – 2019 vychází hodnoty 3,01 %, 6,01 % a 4,6 % a model lze tedy prohlásit za funkční. Křivky reálných dat jsou – s ohledem na zadání konkrétních reálných hodnot pouze do roku 2019 – v dalších letech pro nedostatek dat konstantní (z toho důvodu se také křivky následně rozcházejí).

- "počet uživatelů" hodnota MAPE 3,01 %



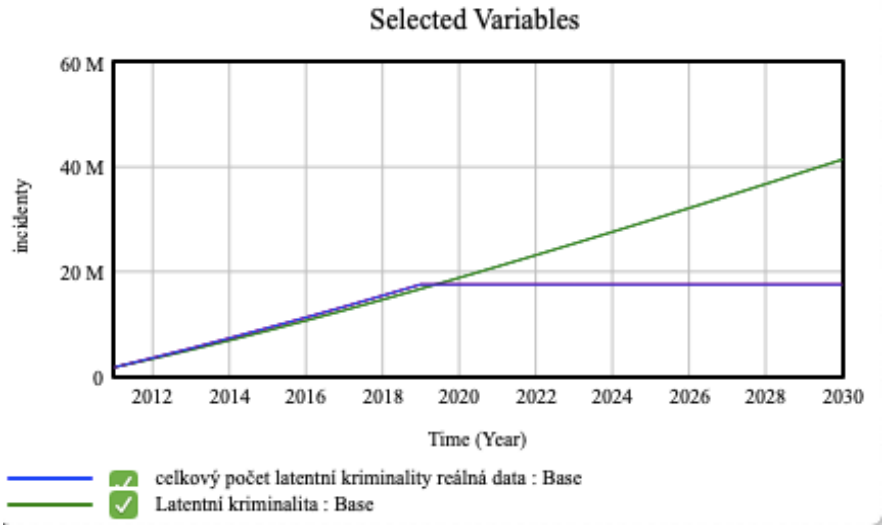
Obrázek č. 11 – Porovnání reálných dat se simulovanými (počet uživatelů) v letech 2011-2019

- počet "oznámených trestných činů" hodnota MAPE 6,01 %



Obrázek č. 12 – Porovnání reálných dat se simulovanými (počet oznámených TČ) v letech 2011-2019

- počet "latentní kriminality" hodnota 4,6 %



Obrázek č. 13 – Porovnání reálných dat se simulovanými (latentní kriminalita) v letech 2011-2019

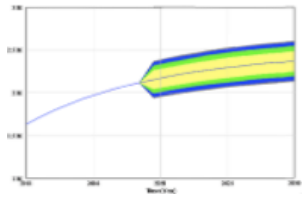
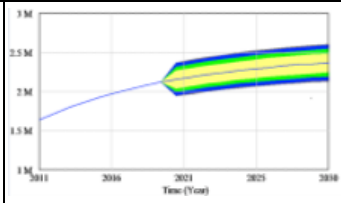
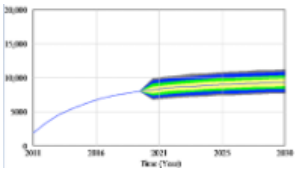
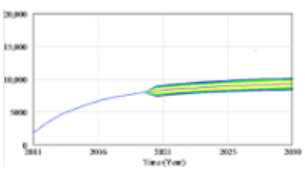
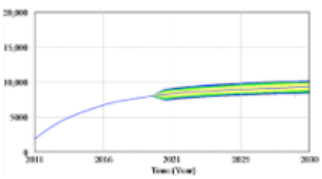
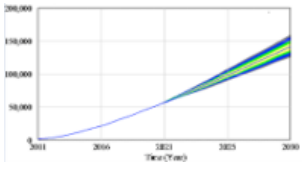
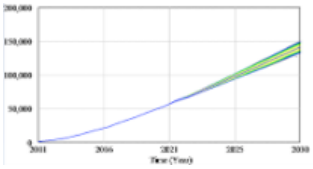
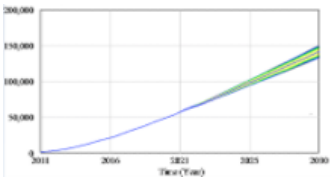
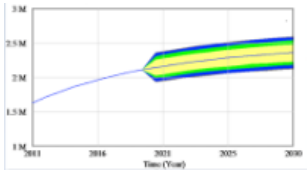
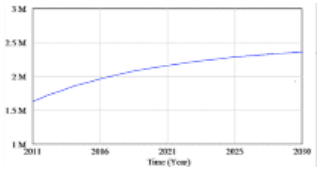
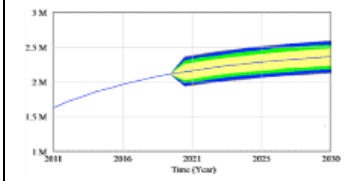
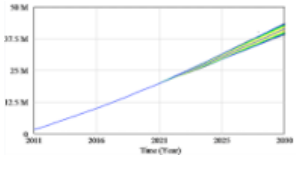
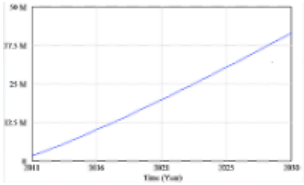
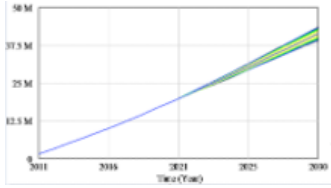
4.5 Simulace SFD modelu do roku 2030

Nejprve byla provedena citlivostní analýza pro změnu proměnných „změna přírůstku bezpečnostních incidentů" a „změna oznamování bezpečnostních incidentů" (obě v základním nastavení mají hodnotu „1") a dále byly vybrány 3 scénáře, ve kterých byl simulován vývoj do roku 2030.

4.5.1 Citlivostní analýza

Byla provedena citlivostní analýza změn vybraných parametrů pro období 2020-2030, umožňující interaktivně zobrazit, jak změny parametrů vstupních proměnných mohou ovlivnit výstupní proměnné. Citlivostní analýza je provedena na principu simulace „Monte

Carlo“ (tedy určení střední hodnoty veličiny, která je výsledkem náhodného děje), kdy program Vensim umožňuje provádět opakované simulace, ve kterých jsou v rámci každé simulace měněny parametry modelu (měněny mohou být pouze konstanty), což umožňuje větší pochopení hranic chování modelu (Ventana Systems, 2010, s. 239 - 242). Citlivostní analýza byla provedena s nastavením - Number of simulations = 1000, Noise Seed = 1234, kdy čísla byla náhodně generována podle rovnoměrného rozdělení pro parametr v rozmezí 0.9 – 1.1. Zároveň byla zvolena možnost „multivariate“ (change all together), která znamená, že pakliže je provedena citlivostní analýza pro více parametrů, dochází k jejich změně najednou. Jedná se o dílčí citlivostní analýzu (testování vlivu několika vybraných parametrů a ne všech vstupních parametrů výpočtu) – v tomto případě pro vliv „změna přírůstku bezpečnostních incidentů“ a „změna oznamování bezpečnostních incidentů“.

Výsledky citlivostní analýzy změny vybraných proměnných			
	kombinace změny obou proměnných	změna oznamování bezpečnostních incidentů	změna přírůstku počtu bezpečnostních incidentů
přibývání počtu bezpečnostních incidentů			
oznamování trestné činnosti			
počet oznámených TČ			
vznik latentní kriminality			
latentní kriminalita			

Obrázek č. 14 - Výsledky citlivostní analýzy

Na obrázku jsou uvedeny výsledky citlivostní analýzy ve zvoleném rozmezí parametru 0.9 – 1.1 v letech 2020 - 2050. V 1. sloupci jsou výsledky v případě zkoumání vlivu obou proměnných - „změna přírůstku bezpečnostních incidentů“ a „změna oznamování bezpečnostních incidentů“. V druhém sloupci jsou výsledky zkoumání vlivu proměnné „změna oznamování bezpečnostních incidentů a ve 3. sloupci jsou výsledky zkoumání vlivu proměnné „změna přírůstku počtu bezpečnostních incidentů“. Z analýzy je pak zřejmý malý vliv „změny oznamování bezpečnostních incidentů na latentní kriminalitu a její vznik. Naopak vliv změny přírůstku počtu bezpečnostních incidentů je na vznik latentní kriminality velký. U změny obou proměnných (pakliže je jejich vliv uvažován zvlášť) pak není rozdíl co se týče vlivu na oznamování trestné činnosti a tedy i na počet oznámených trestných činů.

4.5.2 Scénáře

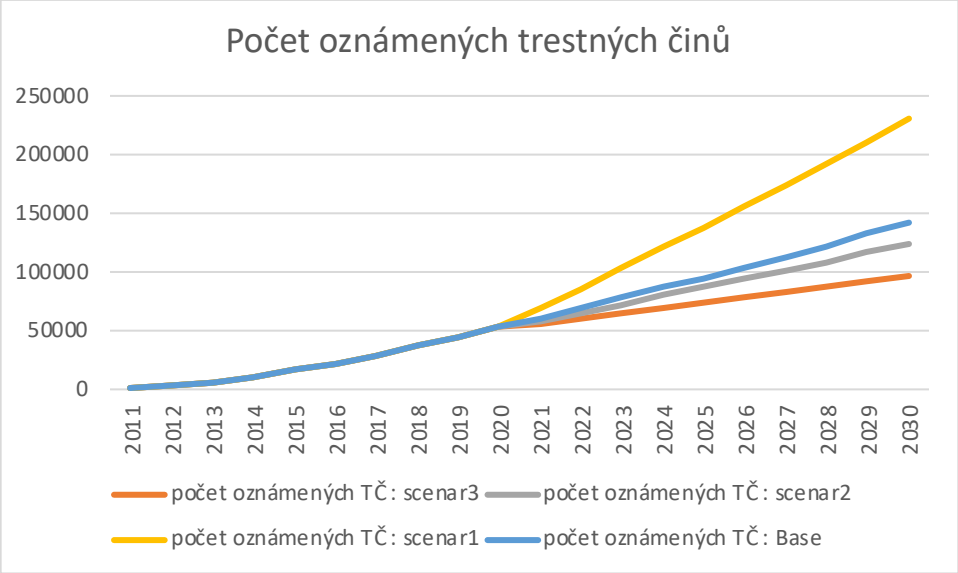
SFD model v zobrazení SyntheSim (viz. obrázek č. 11), umožňuje vidět možnost změny konstantních proměnných (tlačítky se dvěma šipkami do stran), což znamená, že je připraven na případné další upřesnění modelovaných prvků v závislosti na nově dostupných statistických údajích a dalších zjištěných skutečnostech. V současné podobě modelu je možné simulovat zvolený problém s proměnnými, které jsou v době vytvoření modelu známé a dostupné. Pro simulaci modelu byla vybrána proměnná „změna přírůstku počtu bezpečnostních incidentů“, kdy změnou byl simulován její vliv na hodnotu cílových stavů „počet oznámených TČ“ a „Celková škoda“. Simulace byla provedena s využitím počátečních hodnot stavových proměnných v roce 2011, ale jak již bylo uvedeno výše, do roku 2020 se jejich vliv v systému neprojeví. Hodnoty do roku 2019 jsou zachovány a změna se týká pouze období od roku 2020 do roku 2050. Pro simulaci modelu byly vybrány 3 scénáře vývoje za zvolené období, kdy míra změny proměnné byla zvolena na základě vlastního odhadu k testování hypotetických možností změny.

Proměnná **„změna přírůstku bezpečnostních incidentů“** (v původním nastavení na hodnotě „1“ byla nastavena v rámci scénářů na tyto hodnoty:

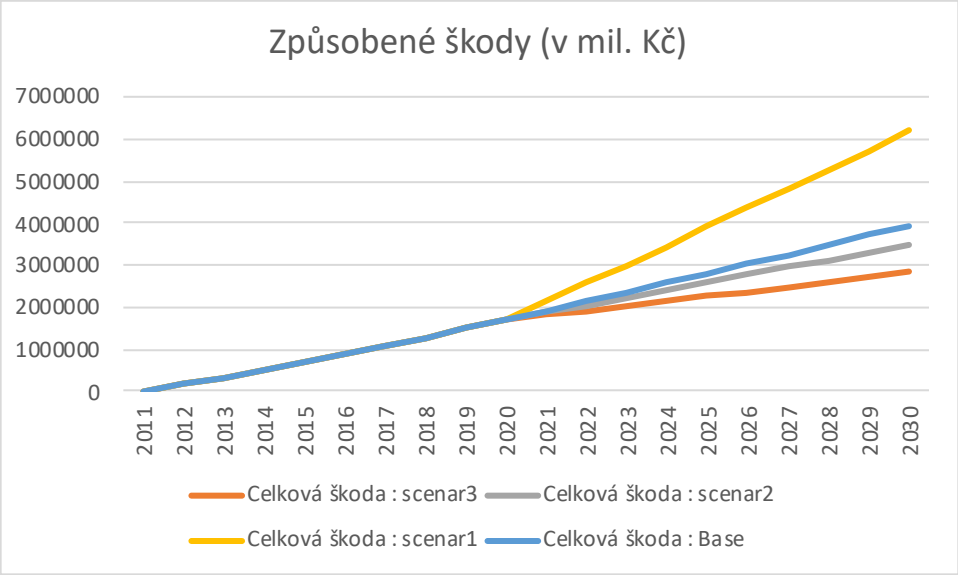
Scénář 1 – změna proměnné z hodnoty 1 na hodnotu 2 – to znamená, že by se míra přibývání počtu bezpečnostních incidentů dvojnásobně zvýšila.

Scénář 2 – změna proměnné z hodnoty 1 na hodnotu 0.8 – to znamená, že by se míra přibývání počtu bezpečnostních incidentů o 20 % snížila.

Scénář 3 – změna proměnné z hodnoty 1 na hodnotu 0.5 – to znamená, že by se míra přibývání počtu bezpečnostních incidentů o 50 % snížila.



Obrázek č. 15 – Vliv změn na "počet oznámených trestných činů"



Obrázek č. 16 - Vliv změn na „celkový počet způsobených škod“

V rámci simulace stanovených scénářů byl zjištěn vliv změny proměnné na cílové stavové hodnoty. Hodnoty „Base“ jsou v základním nastavení systému, tedy v případě, že by nedošlo ke žádným změnám, další možnosti vývoje jsou vždy označeny číslem scénáře.

5 Zhodnocení a doporučení

Problém kyberkriminality je dynamický komplexní systém, jehož chování je definováno řadou zásadních zpětných vazeb. Z uvedených výstupů je patrné, jakým způsobem lze aplikovat disciplínu systémové dynamiky na zvolený problém a lze činit závěry o vlivu změny hodnot proměnných na zkoumaný systém. Je tedy možné konstatovat, že aplikace systémové dynamiky na daný problém je velice vhodným řešením. Oproti jiným přístupům umožňuje zvolený model pracovat i s měkkými faktory, například motivace, důvěra, atp. Fáze aplikace lze pak shrnout do modelování, abstrahování entit a jejich vztahů, tvorby modelu (systému rovnic s pomocí softwaru) a následně simulace (numerické řešení modelu). Zkoumání výsledku interakce ve složitých systémech je možné přirovnat k řešení soustavy tisíce diferenciálních rovnic. Vzhledem k možnosti využití softwarového nástroje Vensim je však modelování mnohem snazší.

Simulační model pak slouží pro účely citlivostní analýzy, ze které vyplývá, jak se která změna proměnných „změna přírůstku bezpečnostních incidentů“ a „změna oznamování bezpečnostních incidentů“ v systému projevuje. Obě proměnné mají v rámci základního nastavení systému hodnotu „1“ – tedy průměrný vliv na základě historických dat. Jak je patrné z CLD modelu, na proměnnou **oznamovat bezpečnostní incidenty** má vliv činnost policie (ochota - přijímat trestní oznámení apod., počet odsouzených pachatelů), ale i opatření mimo trestněprávní rovinu – osvěta, zlepšení opatření k zajištění kyberbezpečnosti, výše způsobených škod a bezpečnostních incidentů. Stejně tak na **přírůstek počtu bezpečnostních** incidentů, kdy jejich počet narůstá nejen s počtem uživatelů online a jejich aktivit v kyberprostoru, ale také s počtem zvyšujícího se počtu zranitelností online (tyto jsou snižovány v případě zvýšení kvality opatření k zajištění kyberbezpečnosti – tedy určitou osvětou, která je ovlivněna i kvalitní prací Policie ČR). Do modelu by tedy bylo možné dále přidat zpětnovazební smyčky, které tyto – konstantní – hodnoty ovlivňují. Z výsledků citlivostní analýzy je pak patrná velká citlivost vzniku latentní kriminality na změnu přírůstku počtu bezpečnostních incidentů. Naopak vliv změny oznamování bezpečnostních incidentů je na latentní kriminalitu minimální. Na počet oznámených trestných činů pak mají obě zvolené proměnné přibližně stejný vliv. Otázkou je, zda náklady na prevenci jsou nižší, než náklady na trestní řízení. S ohledem na možné různé průběhy trestního řízení (počet zadaných znaleckých posudků, náklady na mezinárodní spolupráci, apod. jsou náklady na trestní řízení velice těžko vyčíslitelné. 1 % oznámených trestných činů se také liší od 1 %

neoznámených incidentů. Zatímco k oznámení dochází především v závažnějších případech, v naprosté většině ve chvíli, kdy dojde ke způsobení škody, u bezpečnostních incidentů (tak jak jsou vnímány ve statistikách) nemusí ke vzniku primární škody vůbec dojít.

Změny právě v hodnotě „změna bezpečnostních incidentů“ i míra změny byly zvoleny na základě zjištěného k simulaci sestaveného modelu. Byly vybrány tři reprezentativní scénáře, avšak v rámci dynamického modelu je možné nejen nastavit zvolené hodnoty jiným způsobem, ale také v jiné kombinaci. Například upravit změnu proměnné „míra přibývání počtu uživatelů“ v případě, že by došlo ke zvolňování jejich růstu. Dále je možné v rámci sestaveného modelu zkoumat vliv dalších proměnných na systém (například průměrnou škodu na skutek, míru přibývání počtu bezpečnostních incidentů, apod. Model byl však využit k simulaci tří reprezentativních scénářů, kdy byl zkoumán vliv proměnné „změna přírůstku bezpečnostních incidentů“ konkrétně z hodnoty 1 na hodnoty 2, 0.8 a 0.5. Ze simulace je patrný nárůst počtu oznámených trestných činů ve scénáři č. 1. S ohledem na tento výsledek se dostáváme k diskuzi nad kapacitami Policie ČR přijímat takové množství trestních oznámení. Stejný případ nastává, pokud dojde ke zvýšené míře oznamování bezpečnostních incidentů (i při nezměněné míře přírůstku bezpečnostních incidentů), byť jak již bylo uvedeno větší míra dat dostupných Policii poskytne lepší podklady pro objasňování trestné činnosti, tato změna musí být doprovázena interními změnami ve struktuře Policie ČR, resp. její prací s informacemi, možnostmi propojení poznatků nejen z trestních oznámení, ale také z veřejných zdrojů. Z modelu vyplývá, že existuje vliv mezi mírou škod a motivací oznamovat trestné činy. Jak je patrné ze simulací, ve všech případech dochází k enormnímu nárůstu celkových škod. Ačkoliv jsou škody za jednotlivé bezpečnostní incidenty vypočítány dle průměrné škody na oznámený trestný čin a jedná se tedy spíše o maximální hranici, jelikož dochází k oznámení především v případech, ve kterých byla způsobena větší škoda, stále se jedná o enormní částky. Někteří autoři uvádějí, že osvěta může ušetřit až 82 % nákladů na kyberkriminalitu (Crane, 2020). Z výsledků simulace scénářů je patrná změna sklonu křivky u zvolených scénářů dle vlivu změny proměnné na cílové proměnné, reprezentující vztah mezi cestami možného budoucího vývoje. Model je tedy ukázkou toho, jak je možné přístup systémové dynamiky využít. Jakýkoliv model je určité zjednodušení reality a navrhované parametry a stavební bloky by pak bylo vhodné rozšířit současně s dalším výzkumem. Samotné údaje jsou pouze reprezentativní a vždy mohou být upraveny, aby lépe kvantifikovaly reálné podmínky a stav věcí. Rozšíření modelu by především mohlo mít za cíl doplnit a kvantifikovat zpětnovazební

smyčky tak, jak jsou uvedeny v CLD modelu. Například to, že odsouzení pachatelé (tedy objasněné trestné činy[12]) mohou znamenat návratnost způsobených škod a tím větší motivaci oznamovat trestnou činnost. Rozhodující však nemusí být vždy výsledné hodnoty proměnných, ale pravidla, podle kterých jsou prováděna rozhodnutí (Krejčí, Kvasnička, 2014). Efektivní odpověď na rizika plynoucí ze vzrůstajícího počtu kyberkriminality vyžadují především lepší osvětu v soukromém sektoru a ve státní správě. Například i formou cvičení - v roce 2019 bylo provedeno společné cvičení NÚKIB a NCOZ (NÚKIB, 2020, s. 2). Stejně tak opatření k zajištění kyberbezpečnosti a osvěta znamenají, že osoby jsou více poučené, čímž se snižuje se riziko selhání lidského faktoru (který je často tím nejslabším článkem), zároveň jsou uživatelé poučení jak a jaká zajistit data pro orgány činné v trestním řízení, kterým to přinese značné usnadnění práce (resp. bude znamenat nízkou hladinu ztráty důkazního materiálu). Kvalitní a „úspěšné“ trestní řízení pak znamená větší motivaci policistů i uživatelů oznamovat incidenty. Motivace policistů má velký vliv na jejich přístup k osobám, které se na služebny Policie ČR dostavují s trestním oznámením. Jakmile dochází k nepříjemné zkušenosti, jsou demotivováni příště s policií spolupracovat (hlavně v případech malých škod – například drobných nákupů na podvodných e-shopech, apod.). Míru objasněnosti a tedy i snižování počtu kyberkriminality pak snižuje i fakt, že čím více dat má Policie ČR k dispozici, tím větší pak je možnost jejich analýzy. Jak bylo zmíněno v teoretické části, kyberprostor dnes umožňuje páchat útoky z druhé strany světa, avšak zároveň dochází ke zlepšování mezinárodní spolupráce a poznatky z jedné země je možné předat do jiné, ze které pachatel trestnou činnost páchá. Jak vyplývá ze zjištěného, na celý systém má vliv motivace oznamovat trestnou činnost. Je nutné změnit vnímání, že trestní oznámení je pouze ztrátou času a nevede k nápravě. Větší angažovanost uživatelů internetu, zvlášť když tak velké množství jich uvádí, že setkalo s bezpečnostním incidentem, by umožnilo snížit případy latentní kriminality. Jedním z prvků motivace je pak snadná cesta hlášení bezpečnostních incidentů. V roce 2012 byla Policií ČR spuštěn činnost tzv. „hotline PČR“, za účelem hlášení závadového obsahu a aktivit v síti Internet, bohužel její činnost byla v roce 2018 ukončena (Policie ČR, 2019, s. 30). Tato aktivita je například stále funkční v jiných zemích – např. ve Velké Británii – kde při online oznámení a registraci je možné

[12] Ne každý objasněný trestný čin (tedy situace sdělení obvinění osobě dle § 160 odst. 1 trestního řádu) končí po soudním řízení odsouzením pachatele.

dále sledovat postup v rámci trestního řízení[13]. Čím více incidentů bude totiž zadokumentováno, tím více bude možné incidenty analyzovat a zajistit potřebné materiály k identifikaci pachatelů a prokázání spáchání trestného činu.

[13] na webové stránce britské policie - Reporting Fraud and Cybercrime - https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

6 Závěr

Model vychází z logiky systémové dynamiky a slouží ke zkoumání efektu proměnných na míru kyberkriminality v České republice. Tvorba modelu pak umožňuje nejen takovouto simulaci při změnách zvolených proměnných, ale také zjištění, které proměnné mohou mít na celý proces vliv. I když se jedná o určité zjednodušení (jako u jakéhokoliv modelu, který pouze reprezentuje realitu), může být perspektivním nástrojem pro pochopení systému, případně pro zkvalitnění rozhodovacích procesů.

Práce také ukázala, jak model systémové dynamiky, může být užitečný nejen v prostředí businessu, ale také pro rozhodování v rámci státní správy, kdy umožní podpořit správná strategická rozhodnutí tím, že na teoretické bázi ukáže chování systému dříve, než dojde k implementaci změn v praxi. V rámci bakalářské práce byly sestaveny dva modely systémové dynamiky – CLD a z něj vycházející model SFD, který byl pak dále otestován na reálných datech. Do modelu odpovídající reálným datům byly uměle vloženy parametry za účelem odhalení odezvy systému. Při simulaci pro období 2020-2030 byla dynamicky měněna hodnota proměnných „změna přírůstku bezpečnostních incidentů“ a „změna oznamování bezpečnostních incidentů“ a s využitím citlivostní analýzy byl ukázán vliv této změny. Dále byly simulovány tři scénáře s různým nastavením proměnné „změna přírůstku bezpečnostních incidentů“ tak, aby bylo možné zkoumat změny systému, resp. vliv na zkoumání změny stavu cílových proměnných (počet oznámených trestných činů a počet škod), které by při současném nastavení systému (i při simulovaném vývoji) značně rostly. Angažovanost uživatelů internetu může výrazně snížit počet případů bezpečnostních incidentů, jelikož vliv motivace na oznamování těchto incidentů (a tím pádem i jejich oznamování) orgánům činným v trestním řízení může zlepšit schopnosti Policie ČR zajišťovat relevantní data a napomoci objasňovat trestnou činnost, což by mělo mít zpětně za následek snížení počtu incidentů a snížení přírůstku kyberkriminality v ČR.

7 Seznam použitých zdrojů

ACCENTURE, 2019. *Ninth Annual Cost of Cybercrime Study* [online]. 6. března 2019. [cit. 2020-09-10] Dostupné z: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

BIDGOLI, Morvareed, GROSSKLAGS, Jens, 2016. End User Cybercrime Reporting: What We Know and What We Can Do to Improve It. 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) [online]. 17. listopadu 2016. [cit. 2020-09-09]. Dostupné z: https://www.in.tum.de/fileadmin/w00bws/cybertrust/papers/2016-ICCCF-Bidgoli.pdf

COETZEE, Lezanie, 2015. *Modelling Drug Abuse and Drug-related Crime: A Systems Approach.* Stellenbosch: Stellenbosch University, MSc. práce. [cit. 2020-08-09]. Dostupné z: https://www.researchgate.net/publication/317240149_A_Systems_Dynamic_Model_for_Drug_Abuse_and_Drug-Related_Crime_in_the_Western_Cape_Province_of_South_Africa

CRAIGEN, Dan a kol., 2014. Defining Cybersecurity. *Technology Innovation Management Review* [online]. Dostupné z: http://doi.org/10.22215/timreview/835

CRANE, Casey, 2020. *The Definitive Cyber Security Statistics Guide for 2020* [online]. 14.května 2020. [cit. 2020-10-10]. Dostupné z: https://www.thesslstore.com/blog/cyber-security-statistics/

DRMOLA, Jakub, 2014. Systémová dynamika jako nástroj pro výzkum bezpečnosti. *Obrana a strategie* [online], roč. 14, č. 1. [cit. 2020-08-10]. ISSN 1802-7199. Dostupné z: https://www.obranaastrategie.cz/cs/aktualni-cislo-1-2014/clanky/systemova-dynamika-jako-nastroj-pro-vyzkum-bezpecnosti.html

EUROPOL, 2019. *Internet Organised Crime Threat Assessment (IOCTA) 2019.* [online]. 09.10.2019. [cit. 2020-09-09]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32008L0114

EUROPOL, 2020. *Internet Organised Crime Threat Assessment (IOCTA) 2020.* [online]. 05.10.2020. [cit. 2020-09-09]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32008L0114https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

FORRESTER, Jay. W., 1995. *Counterintuitive Behavior of Social Systems* [online]. 1995. [cit. 2020-10-09]. Dostupné z: http://static.clexchange.org/ftp/documents/system-dynamics/SD1993-01CounterintuitiveBe.pdf

GILLILAND, Michael, 2010. Forecasting FAQs. *The Business Forecasting Deal: Exposing Myths, Eliminating Bad Practices, Providing Practical Solutions* [online]. SAS Institute, Inc. 2010. [cit. 2020-11-11]. Dostupné z: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119199885.app1

GOODMAN, Marc. D., 1997. Why the Police Don't care about computer crime. *Harvard Journal of Law & Technology* [online], roč. 10, č. 3. [cit. 2020-09-09]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.journals/hjlt10&div=21&id=&page=

GRAHAM, Amanda a kol., 2019. Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal* [online]. 17. prosince 2019. [cit. 2020-08-09]. Dostupné z: https://www.emerald.com/insight/content/doi/10.1108/PIJPSM-07-2019-0115/full/html

GŘIVNA, Tomáš a kol., 2014. *Kriminologie - 4., aktualizované vydání*. Praha: Wolters Kluwer, a.s., 536 s. ISBN 978-80-7478-615-0

HUSÁK, Ondřej, 2020. Bezpečnostní experti bijí na poplach, nárůst phishingových podvodů je alarmující. *Novinky* [online]. 12.10.2020. [cit. 2020-13-10] Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/bezpecnostni-experti-biji-na-poplach-narust-phishingovych-podvodu-je-alarmujici-40338601

INSTITUT PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCI, 2019. *Škody působené kybernetickou kriminalitou* [online]. [cit. 2020-13-13]. Dostupné z: http://www.ok.cz/iksp/docs/450.pdf

INTERPOL, 2020. *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. 4. srpna 2020 [online]. [cit. 2020-10-05]. Dostupné z: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

ISO/IEC 2382-8:1993, 2001, zavedena v ČSN ISO/IEC 2382-1 (36 9001) *Informační technologie – Slovník – Část 8: Kontrola, neporušenost a bezpečnost*. Praha: Český normalizační institut.

ITU - International Telecommunication Union. *Statistics* [online]. [cit. 2020-10-09]. Dostupné z:. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

KAISER, Gunther, 1994. *Kriminologie - 1. vydání*. Praha: C.H. Beck. 267 s. ISBN 80-7179-002-8

KHAIR Ummul a kol., 2017. Forecasting Error Calculation with Mean Absolute Deviation and Mean Absolute Percentage Error. *Journal of Physics: Conference Series* [online], č. 930. [cit. 2020-15-11]. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/930/1/012002/pdf

KHALID, Saeed a PAVLOV, V. Oleg., 2006. *Dynastic cycle: A generic structure describing resource allocation in political economies, markets and firms* [online]. 9. ledna 2006. [cit. 2020-08-08]. Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.504.7556&rep=rep1&type=pdf

KOLOUCH, Jan, 2016. *Cybercrime.* Praha: CZ.NIC, z.s.p.o, 522 s. ISBN 978-80-88168-15-7

KREJČÍ, Igor a KVASNIČKA, Roman, 2014. *Systémová dynamika I*. Praha: Česká zemědělská univerzita v Praze. 2014, 67 s. ISBN 978-80-213-2478-7

KSHETRI, Nir, 2005. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 2005, roč. 11, č. 4, s. 541-562. ISSN 1360-2241

LANE, David. C., 2007. The power of the bond between cause and effect: Jay Wright Forrester and the field of system dynamics. *System Dynamics Review* [online], 2007, roč. 23, č. 2-3. [cit. 2020-08-08]. Dostupné z: https://onlinelibrary.wiley.com/doi/abs/10.1002/sdr.370

LEE, Soochang a JUNG, Wooyeol, 2017. System Dynamics Approach to Ability of the Police for Solving Crime : Testing the Effect of Civic Cooperation with the Police. *International Journal of Advanced Culture Technology* [online], roč. 5, č. 1. [cit. 2020-10-10]. Dostupné z: https://www.researchgate.net/publication/317714318_System_Dynamics_Approach_to_Ability_of_the_Police_for_Solving_Crime_Testing_the_Effect_of_Civic_Cooperation_with_the_Police

LOVE, Terence, 2009. *Complicated and Complex Crime Prevention and the 2 Feedback Loop Law* [online]. [cit. 2020-08-10]. Dostupné z: https://www.love.com.au/docs/2009/idoc09-tl.htm

MACDONALD, Rod a MOJTAHEDZADEH, Mohammad, 2014. *Criminal Justice Simulation Model (CJSIM): Using a Simulation Model to Examine the Allocation of Technology to Improve the Criminal Justice System* [online]. New York: University of Albany. [cit. 2020-11-11]. Dostupné z: https://www.researchgate.net/publication/242229633_Criminal_Justice_Simulation_Model_CJSIM_Technology_and_the_Flow_of_Criminals_in_the_Criminal_Justice_System

MILDEOVÁ, Stanislava a VOJTKO, Viktor, 2008. *Systémová dynamika – 2. přeprac. vydání*. Praha: Oeconomica, 150 s. ISBN 978-80-245-1448-2

MILDEOVÁ, Stanislava, 2014. Systémová dynamika a její modely jako součást Competitive Intelligence. Acta Informatica Pragensia [online], roč. 3, č. 3, s. 288-294. [cit. 2020-08-09]. Dostupné z: https://www.researchgate.net/publication/287725966_Systemova_dynamika_a_jeji_modely_jako_soucast_Competitive_Intelligence

MURPHY, Kristina, CHERNEY, Adrian, 2001. Fostering cooperation with the police: How do ethnic minorities in Australia respond to procedural justice-based policing? *Australian & New Zealand Journal of Criminology* [online], roč. 44, č. 2, s. 235-257. [cit. 2002-09-09]. Dostupné z: https://www.researchgate.net/publication/239770190_Fostering_Cooperation_with_the_Police_How_do_Ethnic_Minorities_in_Australia_Respond_to_Procedural_Justice-Based_Policing

NÚKIB, 2020. *Zpráva o stavu kybernetické bezpečnosti ČR – rok 2019* [online]. 18.09.2020. [cit. 2020-10-10]. Dostupná z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

OECD, 2013. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from 1980 and its revision in 2013* [online]. 2013. [cit. 2020-09-09]. Dostupné z: http://www.oecd.org/sti/ieconomy/privacy.htm

POLICIE ČR, 2019. *Výroční Zpráva NCOZ 2018* [online]. [cit. 2020-09-09]. Dostupné z: https://www.policie.cz/clanek/zprava-o-cinnosti-ncoz-za-rok-2018.aspx

POLICIE ČR, 2020. *Výroční Zpráva NCOZ 2019* [online]. [cit. 2020-09-09]. Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-vyrocni-zprava-ncoz-2019.aspx

POLICIE ČR. nedatováno/a, *Kyberkriminalita* [online]. [cit. 2020-08-08]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

POLICIE ČR. nedatováno/b, *Statistika kyberkriminality* [online]. [cit. 2020-03-10]. Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

QIAN, Ying a kol., 2012. Managing information security risks during new technology adoption. *Computers and Security.* [online]. 8 August 2012, s. 859-869. [cit. 2020-11-11]. Dostupné z: https://www.researchgate.net/publication/257006511_Managing_information_security_risks_during_new_technology_adoption

RADA EU, nedatováno. *Cybersecurity in Europe: stronger rules and better protection* [online]. [cit. 2020-12-10]. Dostupné z: https://www.consilium.europa.eu/en/policies/cybersecurity/

SKARIN, Bruce a kol., 2009. Modeling the Cycles of Gang and Criminal Behavior: Understanding the Social and Economic Influences. *Proceedings of the 27th International System Dynamics Society Conference* [online]. [cit. 2020-09-10]. Dostupné z:

https://www.researchgate.net/publication/317240149_A_Systems_Dynamic_Model_for_Drug_Abuse_and_Drug-Related_Crime_in_the_Western_Cape_Province_of_South_Africa

STERMAN, John, 2000. *Business Dynamics: systems Thinking and Modelling for a Complex World*. Boston: McGraw-Hill. 982 s. ISBN 978-007238915

SWINHOE, Dan, 2019. Why businesses don't report cybercrimes to law enforcement. *CSO* [online]. 30. května 2019. [cit. 2020-05-10]. Dostupné z: https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

SWINHOE, Dan, 2020. The 15 biggest data breaches of the 21st century. *CSO* [online]. 17. dubna 2020. [cit. 2020-02-11]. Dostupné z: https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances

ŠUSTA, Marek, 2015. *Průvodce systémovým myšlením*. Praha: Proverbs. a.s., 136 s. ISBN 978-80-260-7602-5

ŠUSTA, Marek, KOSTROŇ, Lubomír, 2004. *Úvod do systémové dynamiky pro sociální vědy* [online]. Masarykova univerzita v Brně, Fakulta sociálních studií, Katedra psychologie. [cit. 2020-08-08]. Dostupné z: https://is.muni.cz/el/1431/jaro2010/M8115/um/UvodSD.pdf

THOMAS, Karl, 2015. *The sad stats on state of cybersecurity: 70% attack go unchecked* [online]. [cit. 2020-08-08]. Dostupné z: https://www.welivesecurity.com/2015/09/09/cybercrime-growing-concern-americans/

VENTANA SYSTEMS, 2010. *Vensim Reference Manual* [online]. Harvard: Ventana Systems [cit. 2020-10-11]. Dostupné z: http://www.vensim.com/documentation.htm

VOJTKO, Viktor, MILDEOVÁ, Stanislava, 2007. *Dynamika trhu jak pochopit síly, které mění trhy, konkurenci a podnikání*. Zeleneč: Profess Consulting. 124 s. ISBN 978-80-7259-052-0

ZOULOVÁ, Lenka, 2020. Hackeři se zaměřují na pacienty s koronavirem. *Novinky* [online]. 27.10.2020. [cit. 2020-11-11]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackeri-se-zamerujina-pacienty-s-koronavirem-40340503

Statistiky Českého statistického úřadu a EUROSTATu (statistický úřad Evropské unie)

Legislativa

Budapešťská úmluva Rady Evropy o kyberkriminalitě (CETS č. 185) ze dne 23. listopadu 2001

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost")

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)"

Zákon č. 141/1961 Sb. ze dne 29. listopadu 1961, o trestním řízení soudním (trestní řád)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zákon č. 40/2009 Sb. ze dne 8. ledna 2009, trestní zákoník

8 Přílohy

Příloha A – Zdrojová data

	uživatelé internetu (%)	počet obyvatel ČR	počet uživatelů online	počet bezpečnostních incidentů (24.7% z počtu uživatel, kteří v posledních 3 měsících použili internet)	počet bezpečnostních incidentů - kumulace	míra růstu počtu uživatelů online dle meziročních rozdílů počtu uživatel online	registrované skutky kyber	počet tč kumulace	latentní TČ - kumulace	objasněné skutky kyber	míra objasňování incidentů (objasněné/registrované)	škody v registrovaných spáchaných skutcích - kyber (v tisicích Kč)
Zdroj	ČSÚ	ČSÚ	ČSÚ	vlastní	vlastní	vlastní	statistiky PČR	vlastní	vlastní	statistiky PČR	vlastní	statistiky PČR
Rok												
2011	65.5	10496672	6875320	1698204	1698204	6.2344	1502	1502	1698204	752	50%	84583
2012	69.5	10509286	7303954	1804077	3502281	1.3088	2195	3697	3502281	1121	51%	100096
2013	70.4	10510719	7399546	1827688	5329969	5.5388	3108	6805	5329969	1495	48%	238345
2014	74.2	10524783	7809389	1928919	7258888	2.1976	4348	11153	7258888	2091	48%	238075
2015	75.7	10542942	7981007	1971309	9230196	1.2710	5023	16176	9230196	2341	47%	349525
2016	76.5	10565284	8082442	1996363	11226560	3.2429	4990	21166	11226560	2558	51%	798515
2017	78.8	10589526	8344546	2061103	13287663	2.7681	5654	26820	13287663	2782	49%	819081
2018	80.7	10626430	8575529	2118156	15405818	0.6525	6815	33635	15405818	3256	48%	744233
2019	80.9	10669324	8631483	2131976	17537795		8417	42052	17537795			
Průměrné míry růstu						2.9017					49%	
ČSÚ - Český statistický úřad, PČR - Policie ČR												

Obrázek č. 17 - Zdrojová data