Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Hrozby z pohledu systémového myšlení se zaměřením na kybernetickou bezpečnost České republiky

Bakalářská práce

Autor: Adam Ostruszka
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Ing. Hana Tomášková, Ph.D.

Hradec Králové duben 2017

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury a dalších informačních zdrojů.

V Hradci Králové dne 28. 4. 2017 Adam Ostruszka

Poděkování:
Děkuji vedoucí bakalářské práce, doc. Ing. Haně Tomáškové, Ph.D. za metodické vedení práce, cenné rady a připomínky a Ing. Ondřeji Doležalovi a Mgr. Jiřímu Havigerovi, Ph.D. za pomoc s tvorbou modelu.

Můj velký dík patří Mgr. Zuzaně Duračinské, resp. sdružení CZ.NIC za představení bezpečnostního týmu CSIRT.CZ a kybernetické bezpečnosti ČR, ochotu a vstřícný přístup při konzultaci práce.

Dále děkuji Mgr. Bronislavu Navrátilovi z Policejního prezidia České republiky za poskytnutí informací o kyberkriminalitě.

V neposlední řadě děkuji MUDr. Janu Pávkovi za pomoc při porovnání systémů kybernetické bezpečnosti a veřejného zdraví.

A na závěr srdečně děkuji svým rodičům za pomoc a podporu při studiu a tvorbě práce.

Anotace

Tato práce se zabývá možnostmi uplatnění systémového myšlení a systémové dynamiky v oblasti kybernetické bezpečnosti.

V první částí nejprve stručně představuje základy systémového myšlení a přístupu, ve druhé analyzuje současný stav kybernetické bezpečnosti a hrozeb v České republice. Ve třetí částí představuje možnosti aplikace systémového myšlení na kybernetickou bezpečnost – shrnuje dosavadní vývoj, analyzuje současný systém a jeho nedostatky a zkoumá systémovost současného přístupu, předvádí možnosti využití systémové dynamiky na příkladu kyberkriminality.

Přínosem práce je tolik potřebná osvěta v oblasti kybernetických hrozeb a bezpečnosti a vybudování základů systémové přístupu v této oblasti, na kterých bude možné dále stavět.

Annotation

Title: Threats from the Perspective of Systems Thinking with Focus on Cyber Security of the Czech Republic

This thesis deals with possibilities of application of systems thinking and system dynamics in the field of cyber security.

The first part briefly presents the basics of systems thinking and approach, the second part analysis current state of cyber security and threats in the Czech Republic. The third part shows the possibilities of application of systems thinking and system dynamics in the field of cyber security – it contains summarization of current development, analysis of the system and its shortcomings, investigation of how systematic the current approach is and an example of using system dynamics in cybercrime prediction.

The benefits of this thesis are the necessary enlightenment of cyber threats and security and building a foundation of systems approach that can be built upon.

Obsah

Seznam obrázků a grafů

1 Úvod

„Množství incidentů v oblasti kybernetické bezpečnosti, ať už úmyslných nebo náhodných, roste alarmujícím tempem a ohrožuje narušení základních služeb, které považujeme za samozřejmé, jako dodávky vody a elektřiny, zdravotní péče, mobilní služby. Hrozby mají různý původ, který může být kriminální, politicky motivovaný, teroristický, sponzorovaný státem, ale také přírodní nebo neúmyslný [1].“

S rozvojem informačních a komunikačních technologií a se stoupající závislostí moderní civilizace na nich, roste množství i význam hrozeb, které představují nebezpeční pro fungování celé společnosti. Prevence, zabezpečení a ochrana před kybernetickými hrozbami představuje do budoucnosti výzvu, které bude třeba čelit. Spolu s rozvojem a nástupem nových technologií neustále přibývají i nové hrozby. Obrana před hrozbami tak představuje velice komplexní problematiku, ke které je třeba odpovídajícím způsobem přistoupit. Jeden z možných způsobů přístupu bude v této práci prozkoumán.

2 Cíle práce a vymezení tématu

Cílem bakalářské práce je představit systémové myšlení a systémovou dynamiku coby přístupy vhodné k řešení komplexnějších problémů a prozkoumat možnosti jeho využití v oblasti kybernetické bezpečnosti, tedy prevence a obrany před kybernetickými hrozbami. To kvůli podstatě systémového přístupu zahrnuje detailní průzkum a analýzu současného stavu kybernetické bezpečnosti na úrovni České republiky. Na základě toho lez sestavit model systému a ověřit, zda a do jaké míry je systémové myšlení aplikováno, případně zda a jak lze jeho aplikací přispět ke zlepšení situace a zvýšení bezpečnosti.

Přestože mnohé kybernetické hrozby se šíří bez ohledu na státní hranice [1], konkrétní hrozby a bezpečnostní potřeby závisí na průmyslové, ekonomické a společenské vyspělosti státu a jeho geopolitické situaci, a na základě toho byla zkoumaná oblast omezena na Českou republiku.

3 Systémy a systémové myšlení

3.1 Systém

Systém bývá intuitivně chápán jako pojem označující uspořádanost nebo organizovanost. První možnou definici pojmu nabízí už sama etymologie slova. *Systém* pochází z latinského *systema*, které má původ v řeckém *sunistánai,* znamenajícím *držet pohromadě*; *zapříčiňovat držení pohromadě.* Slovo samotné je složeninou ze *sun – spolu; dohromady* a *histanai – zapříčiňovat držení; založit; stát* [2] [3].
Českým synonymem pro systém je slovo *soustava*, které významově odpovídá původnímu pojmu.

Akademický slovník cizích slov [4] k pojmu *systém* nabízí následující definice:

1. *soubor jednotlivin navzájem spojených urč. strukturou, sítí vztahů v uspořádaný celek; způsob uspořádání takového vnitřně členitého celku*
2. *uspořádání jednotlivin podle urč. třídicích hledisek v soustavu*
3. *stanovená účelná forma organizace a fungování něčeho*

Obecná teorie systémů [5] nabízí definici:

„Systém je komplex prvků spolu se vztahy mezi nimi a mezi jejich atributy.“

Capra [6] pojem výstižně shrnul s ohledem na vlastnosti:

„Systémem se rozumí integrovaný celek, jehož podstatné vlastnosti vznikají ze vztahů mezi jeho částmi.“

Jiný zdroj [7] definici dále rozšiřuje:

„Systém je soubor interagujících komponent, které společně dosahují nějaké funkcionality. Systémy mohou existovat ve fyzickém světě nebo společenských a politických sférách, nebo mohou být navrženy a vytvořeny explicitně lidmi.“

3.2 Typy systémů

Systémy lze klasifikovat podle různých kritérií [5] [8] [9]:

- Z hlediska vazby systému a okolí lze rozlišovat systémy **otevřené** (řízené), které interagují s okolím a systémy **uzavřené** (volné; neutrální).
- Otevřené systémy lze podle toho, zda obsahují zdroj náhodných poruch, dělit na systémy **deterministické**, ve kterých jsou hodnoty výstupních veličin určeny těmi vstupními a systémy **stochastické** (pravděpodobnostní), ve kterých jsou výstupní veličiny určeny pouze rozdělením pravděpodobností.
- Systémy s konečným počtem vstupních veličin a konečnou strukturou se nazývají **ohraničené**, opakem jsou systémy **neohraničené**.
- Podle hodnot veličin a často také podle toho, jak plyne v systému čas, rozlišujeme systémy **spojité** a **diskrétní**. Diskretizace často vzniká způsobem pozorování spojitých veličin, které vzorkujeme a kvantujeme.
- Systémy, kde všechny veličiny jsou určeny okamžitými hodnotami veličin řídících, označujeme jako **statické** (kombinační; bez paměti). Opakem jsou systémy **dynamické** (sekvenční; s pamětí), kde hodnoty závisí na okamžitých i minulých hodnotách řídících veličin. Jinak řečeno, dynamické systémy se v čase vyvíjí.
- Podle reakce systému na vstupní hodnoty rozlišujeme systémy **bez předvídání** (neanticipativní; kauzální), které reagují jen na minulé a přítomné hodnoty a systémy **s předvídáním** (anticipativní) reagující i na budoucí hodnoty.
- Systémy účelově vytvořené lidskou činností se označují jako **umělé**, opakem jsou systémy **přirozené.**
- **Měkké** systémy, ve kterých hraje důležitou roli lidská složka a jsou zpravidla uchopitelné nejednoznačně nebo vícero způsoby a systémy **tvrdé,** dobře definovatelné, často technické s absencí lidské složky.
- Systémy rozdělitelné do menších podčástí (subsystémů) se označují jako **hierarchické.**
- Abstraktní a konkrétní
- Adaptivní a neadaptivní
- Hmotné, nehmotné a informační
- Reverzibilní

3.3 Struktura a chování systémů

Struktura a chování systému jsou základní vlastnosti všech systémů. Chování systému vyplývá z jeho struktury.

Strukturu systému tvoří prvky a vazby mezi nimi, jinak řečeno struktura je způsob vstupů a výstupů prvků systému [5]. Struktura bývá znázorňována, aby umožnila lepší orientaci v systému a jeho okolí, pomohla vymezit subsystémy, najít a určit závady ve struktuře, respektive ve vymezení systému a chybějících nebo nadbytečných vazbách a aby umožnila při rozboru systému aplikovat matematické vztahy a výpočetní techniku.

Ukázalo se, že mnoho struktur se opakuje v různých systémech na různých úrovních, dokonce v naprosto rozdílných oblastech bádání. Forrester [10] takové struktury označuje jako generické. Pokud jsou dostatečně pochopeny v jedné oblasti, jsou přenositelné i do jiné, jsou také přenositelné mezi minulostí a současností a umožňují tak rychlou orientaci a učení.

Chování systému lze klasifikovat podobným způsobem jako systémy samotné [5]:

- na deterministické a stochastické
- podle doby reagování na chování s okamžitou a se zpožděnou reakcí
- podle změnitelnosti chování
- podle způsobu vývoje
- podle závislosti na čase na statické a dynamické

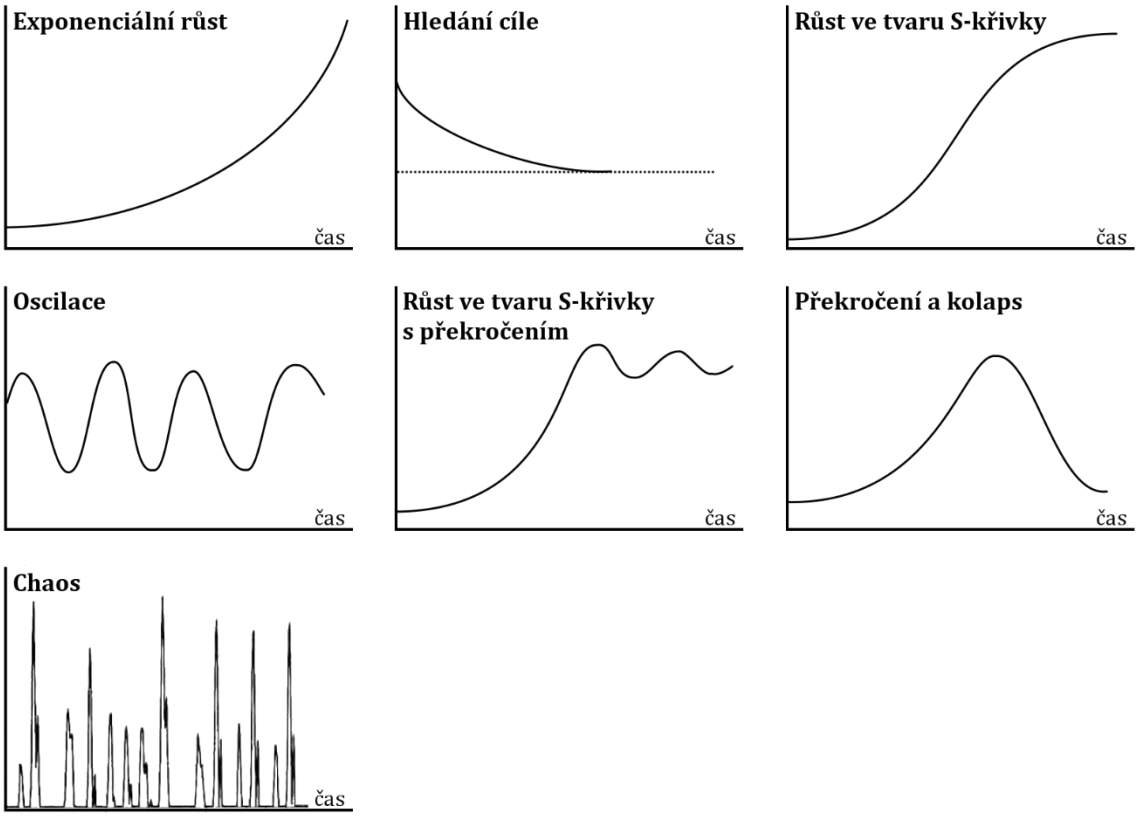
John Sterman [11] mezi rozmanitými druhy dynamického chování systémů vybral a popsal několik základních vzorů, s kterými se lze setkat nejčastěji, a to včetně struktur, které jsou za odpovídající chování zodpovědné. Znalost základních vzorů chování a jejich příčin je nápomocná při modelování systémů.

Vzory zahrnují **exponenciální růst**, tvořený pozitivní (sebeposilující) zpětnou vazbou, **hledání cíle**, tvořené negativní zpětnou vazbou, **oscilace** tvořené negativní zpětnou vazbou s časovými prodlevami.

Komplexnější vzory, jako je **růst ve tvaru S-křivky**, **růst ve tvaru S-křivky s překročením**, **překročení a kolaps** vznikají složením základních vzorů.

Mezi další vzory patří **rovnováha**, zapříčiněná buď tím, že dynamika systému je tak pomalá, že je v daném časovém měřítku neznatelná, nebo zpětnovazebními smyčkami, které udržují stav systému téměř konstantní. Dále sem patří **nahodilost**, která nejčastěji vzniká v důsledku neznalosti nebo přehlížení, než že by byla vlastností systému. Posledním zde

popsaným vzorem je **chaos.** Jde o druh oscilace s neustálým nepravidelným kolísáním, které se nikdy neopakuje. Nepravidelnost je oproti náhodnému chování vlastností systému a není způsobena vnějšími vlivy. Takový systém je navíc velmi citlivý na změnu vstupních podmínek.



Obr. 1: Běžné vzory chování dynamických systémů
Zdroj: převzato a upraveno podle [11]

3.4 Systémový přístup a myšlení

3.4.1 Mechanistický přístup a jeho principy

Systémový přístup je opakem přístupu mechanistického [5], který je historicky starší. Mechanistický přístup je založen na dvou principech:

1) **Redukcionismus**

   Redukcionismus je filozofický názor, že každý systém, jev nebo problém, až už více či méně komplexní, může být rozložen na jednodušší, základní prvky, které jsou snazší na analýzu, pochopení, nebo vysvětlení [11]. Chování celku se vysvětluje pomocí chování jednotlivých částí a celek samotný je chápán jako soubor objektů,

ale vztahy mezi nimi jsou druhotné. Redukcionismus poháněl vědecký pokrok napříč různými obory po staletí a dosud se ve vědě uplatňuje [6].

2) **Mechanismus**

Mechanismus je názor, že veškeré závislosti mezi předměty nebo jevy lze vysvětlit opakovaným použitím kauzality, tedy jednoduchého lineárního vztahu „příčina – následek“ [5]. Forrester poukazuje na to [10], že „*většina lidí přemýšlí lineárním, nezpětnovazebním způsobem.*“ Posloupnost „informace o problému – akce – výsledek“ je známá z tisku, byznysu a politiky. Avšak dodává, že žijeme ve složitém světě, na jehož popsání mechanismus nestačí, ve světě vnořených zpětnovazebních smyček, které jsou přítomné ve všech systémech.

3.4.2 Systémový přístup (myšlení) a jeho principy

Oproti mechanistickému přístupu je systémový přístup založen na tom, že systém nelze pochopit prostřednictvím redukce na menší celky, ale přijetím komplexity, kterou přináší propojení všech částí a jejich vzájemné uspořádání, které je neredukovatelné [12]. Podle Capry [6] „*porozumět věcem systémově znamená doslova umístit je do kontextu, stanovit povahu jejich vztahů*“ a systémové myšlení znamená „porozumění jevům v kontextu většího celku“, což souvisí i s původním významem pojmu *systém*. Barry Richmond [13] definoval systémové myšlení jako „*umění a vědu vyvozování spolehlivých závěrů o chování osvojením rostoucího hlubokého pochopení základové struktury.*“

V souvislosti s tím se často uvádí i výrok, že „*celek je víc než suma jeho částí,*“ jehož původ lze stejně jako původ pojmu *systém* vysledovat až do antického Řecka, v tomto případě k Aristotelovým dílům *Politika* a *Metafyzika*. V dalším rozvoji podobných myšlenek pokračovali Goethe, Kant a Cuvier [6] a později, ve 20. století, na ně navázal filozofický směr zvaný holismus. Kromě filozofie má systémový přístup a myšlení kořeny v mnoha dalších vědách a oborech lidského působení, a to v biologii, antropologii, psychologii, fyzice, managementu a počítačových vědách a spojováno je se jmény mnoha významných vědců 20. století.

Systémový přístup je založen na následujících principech [5] [14] [6] [15]:

1) **Strukturnost a celistvost**

Vzájemná závislost mezi prvky v systému je základem jeho celkové komplexity. Realitu lze strukturovat do sítě relativně stabilních vzájemných spojení a vztahů

dílčích prvků. Pro pochopení určitého jevu je nutno pochopit, čím byl jev vyvolán a co představuje, tedy jakými prvky a vazbami je tvořen. Je nutné zohlednit i vývoj systému v čase a prostoru.

2) **Hierarchičnost a emergence**

   Prvky v systému jsou hierarchicky uspořádané. Jednotlivé úrovně je možné popsat jako nadsystém – systém – subsystém. V různých časových horizontech může mít hierarchičnost různou podobu. Dochází k řetězení následků, změna jednoho prvku se nemusí projevit jen na úrovni daného systému, ale jistě ovlivní i prvky na nižší úrovni a může ovlivnit systém hierarchicky vyšší. Lze pozorovat emergentní vlastnosti, tedy takové, které se objevují na úrovni systému jako celku, a nikoliv jen jeho částí.

3) **Zpětnovazební smyčky**

   Naprostá většina systémů obsahu zpětnou vazbu, tedy zjednodušeně řečeno jev A způsobí jen B, který zpětně ovlivňuje jev A.

4) **Vzájemná závislost systému a prostředí**

   Každý systém je relativně závislý na svém okolí (nadsystému) a zároveň je schopen toto prostředí do jisté míry ovlivňovat. Přestože všechny systémy jsou s okolím propojeny vazbami, v některých případech jsou nevýznamné nebo mají zanedbatelný vliv, takové systémy lze považovat za uzavřené.

Většina práce v duchu systémového myšlení přivedla dohromady vědce z rozmanitých oborů, v mnoha případech jim umožnila přenesení metod z jednoho oboru do jiného nebo práci mezi hranicemi svých oborů, čímž přispívala k rozvoji a učení všech zúčastněných [2]. Systémový přístup našel uplatnění v biologii, ekologii, antropologii, psychologii, fyzice, počítačových vědách a managementu, zdravotní péči, otázkách životního prostředí, fyziologii, závodech ve zbrojení a válkách i výzkumu změn globálního klimatu [11]. Forrester upozorňuje [16], že nedostatečná pozornost je stále věnována ekonomickým záležitostem, budoucnosti systémů sociálního zabezpečení, imigraci, nebo hrozbě politických slibů o stále rostoucí ekonomice a zdravotní péči.

3.5 Systémová dynamika

3.5.1 Definice a počátky vývoje

Systémová dynamika je věda zkoumající chování systémů v čase. Podle Forrestera [17] je nezbytným základem pro efektivní systémové myšlení, podle Richmonda [13] je naopak systémové myšlení základem pro systémovou dynamiku, která představuje jen jeho část. Jak Richmond podotýká, nejsou definice v přímém rozporu, záleží na okolnostech a úhlu pohledu.

Systémová dynamika nabízí sadu nástrojů umožňujících porozumět struktuře a chování komplexních systémů. Je to prakticky orientovaná disciplína, která napomáhá kvalitnějšímu poznávání okolních systémů, zejména těch, ve kterých se vyskytuje vysoká míra detailní a dynamické komplexity [5] [11].

Zakladatelem systémové dynamiky je Jay Wright Forrester z Massachusetts Institute of Technology (MIT), který se jí zabýval od 50. let 20. století po zbytek svého života. Jak vylíčil sám Forrester [18], původně řešil pro firmu General Electric problém spočívající v tom, že v továrnách na domácí spotřebiče v Kentucky se vývoj zaměstnanosti opakoval v tříletých cyklech. Jeden rok se pracovalo na tři a čtyři směny a jiný rok byla polovina zaměstnanců propuštěna pro přebytečnost. Forrester svou, tehdy ještě ručně prováděnou, simulací dokázal, že příčinou nebyly vnější ekonomické cykly, ale vnitropodniková rozhodnutí.

To vedlo k napsání článku a později i knihy *Industrial Dynamics* a vzniku počítačového programu SIMPLE (Simulation of Industrial Management Problems with Lots of Equations). Na sklonku 60. let se systémová dynamika rozšířila i do dalších států. Forrester na základě spolupráce s bývalým Bostonským starostou Johnem F. Collinsem představil v knize *Urban Dynamics* model dynamiky města s ohledem rozvoj zaměstnanosti, kriminalitu a nízkonákladové bydlení jako ghetta, slumy atp. Model je poměrně rozsáhlý, podle Forrestera jeho plné pochopení zabere 2–5 hodin. Tato práce přivedla Forrestera k dalším modelům dynamických sociálních systémů, popsaných v pracích *World Dynamics* a *Limits to Growth*, které byly v době vzniku, podobně jako mnoho dalších vědeckých průlomů, považovány za kontroverzní a vyvolaly mediální pozdvižení.

Forrester s nadhledem shrnul dosavadní vývoj [16] a uvedl, že během prvních padesáti let existence systémové dynamiky se podařilo vytvořit základnu, na které je nutné dále stavět, podařilo se ukázat důležitost porozumění složitým systémům v přírodě a oblastech lidského působení. Systémová dynamika se rozšířila do mnoha směrů, avšak zatím pouze ve velmi malé míře.

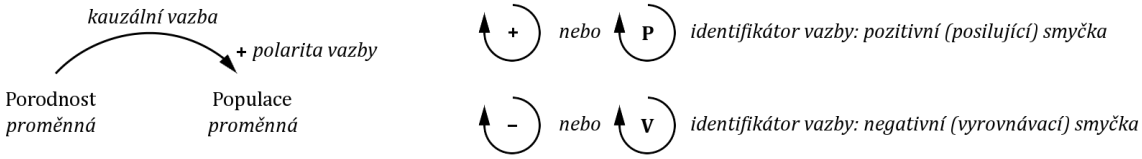
Výuka systémového přístupu a dynamiky se zvolna rozšiřuje z univerzit i na střední a základní školy, ačkoliv stále chybí studijní obory věnované pouze systémům a výuka systémový dynamiky se soustředí hlavně na využití v managementu – poli, kde původně vznikla. Ostatním polím využití, např. interní medicíně, ekonomii nebo politice, se dostává podstatně menší pozornosti. Do budoucna bude podle Forrestera potřeba soustředit se na další rozšiřování pole působnosti systémové dynamiky a na její maximální praktické využití v řešení skutečných problémů.

3.5.2 Nástroje pro modelování systémů

Struktura a chování systémů se znázorňuje pomocí obecně srozumitelných grafických symbolů v několika druzích diagramů, z nichž dva nejpoužívanější jsou představeny níže.

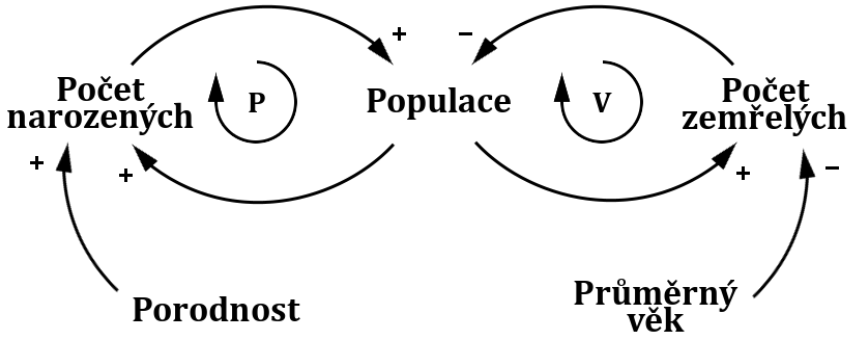
3.5.2.1 Příčinný smyčkový diagram (Casual Loop Diagram)

Příčinné smyčkové diagramy mohou rychle a výstižně zachytit mentální modely, hypotézy o příčinách dynamiky a znázornit hlavní zpětné vazby, které se ve zkoumané oblasti povedlo rozeznat, tzn. mohou tedy dobře zachytit strukturu systému.
Znázorňování smyčkových diagramů se řídí jednoduchými, ale přesnými pravidly.
Prvky systému, proměnné, se znázorňují jako slova, vazby prvků jako šipky určující kauzální (příčinné) vztahy. Každé vazbě je přiřazena polarita, buďto pozitivní (+) nebo negativní (-), která ukazuje, jakým způsobem jsou proměnné ovlivňovány.
Pro zvýraznění důležitých zpětnovazebních smyček je vhodné přidat identifikátory smyček, které ukazují, zda je smyčka pozitivní (sebeposilující) nebo negativní (vyrovnávací) [11].



Obr. 2: Klíč ke čtení příčinných smyčkových diagramů
Zdroj: převzato z [11]

Jednoduchý příklad se dvěma zpětnovazebními smyčkami mezi populací a porodností a mezi populací a úmrtností může vypadat takto:



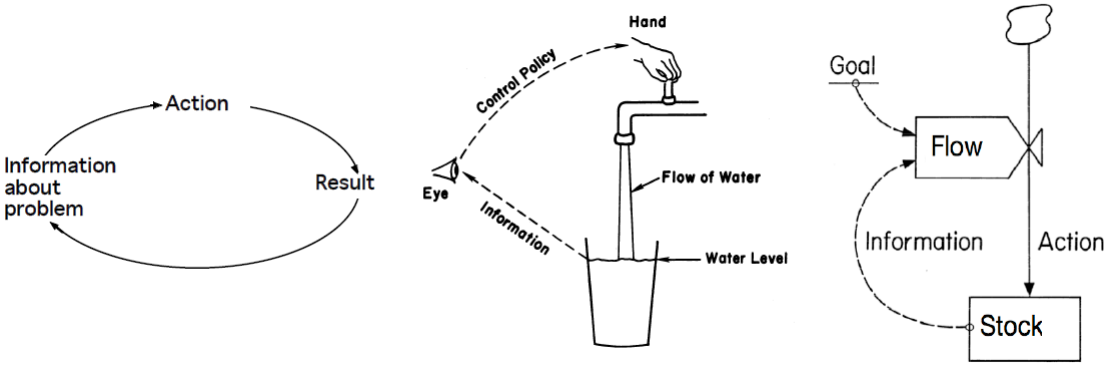
Obr. 3: Příklad jednoduchého příčinného smyčkového diagramu
Zdroj: převzato z [11]

3.5.2.2 Diagram hladin a toků (Stock and Flows Diagram)

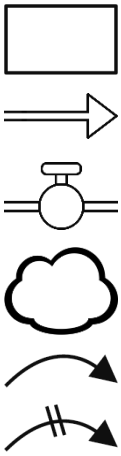
Příčinný smyčkový diagram dobře slouží při návrhu systému a rozpoznání klíčových závislostí, nestačí však na zachycení chování systému, tedy vyjádření aktuální hodnoty proměnných a jejich vývoje v čase [5].

Na rozdíl od příčinného smyčkového diagramu rozlišuje diagram hladin a toků dva druhy proměnných, *hladiny* (stocks) a *toky* (flows). Hladinou se rozumí počet, úroveň, nashromáždění nebo objem. Hladiny dávají systému setrvačnost, paměť a vytvářejí časová zpoždění tím, že hromadí rozdíl mezi přítokem a odtokem. Tokem se rozumí změna ovlivňující hodnoty hladiny [10], [11].

Nemusí být vždy jasné, jaká veličina představuje hladinu a jaká tok, tyto nejasnosti často vedou k podcenění časových zpoždění a krátkodobému zaměření [11].



Obr. 4: Přechod od příčinného smyčkového diagramu přes hydraulickou metaforu k diagramu hladin a toků
Zdroj: převzato z [10]



hladina:
entita, která se během času zaplňuje nebo vyprazdňuje

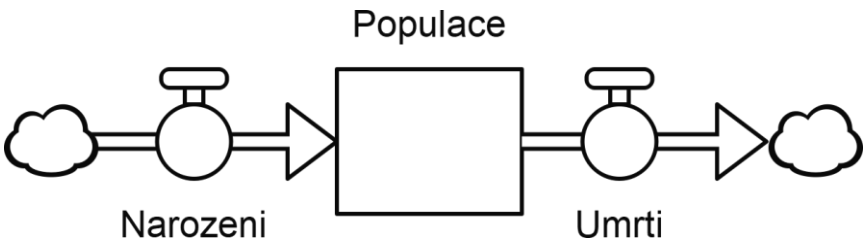
tok:
přesun mezi hladinami
ventil:
regulátor toku

mrak:
zdroj mimo hranice modelu

kauzální vazba

kauzální vazba se zpožděním

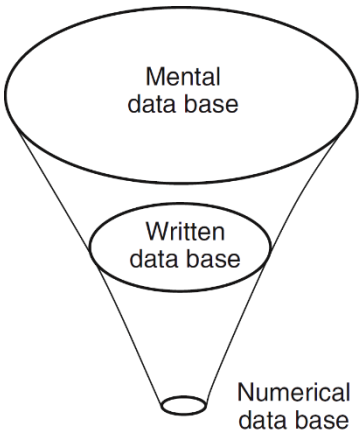
Obr. 5: Klíč ke čtení diagramů hladin a toků
Zdroj: upraveno podle [7]



Obr. 6: Příklad jednoduchého diagramu hladin a toků
Zdroj: upraveno podle [11]

3.5.3 Modelování systému

Podle Forrestera [10] by modely měly být sestavovány ze všech dostupných informací, včetně mentálních modelů a psaných i číselných informací, které se na dostupných informacích podílejí jen nepatrnou částí. Výsledkem analýzy (simulace) hotového modelu by mělo být zlepšení mentálních modelů.



Obr. 7: Zdroje informací
Převzato z [10]

Přechod od mentální modelu k počítačovému Forrester rozdělil do 4 kroků:

1) **Explicitně popsat mentální model**
   Vytvořit model bez logických nesouladů, s jasně definovanými proměnnými, jednotkami a rovnicemi.

2) **Prozkoumat nedostatky**

   Při první simulaci se zpravidla odhalí absurdní výsledky a řada nedostatků.

3) **Prozkoumat důsledky**

   Po odladění model začne odhalovat nové chování a skutečnosti.

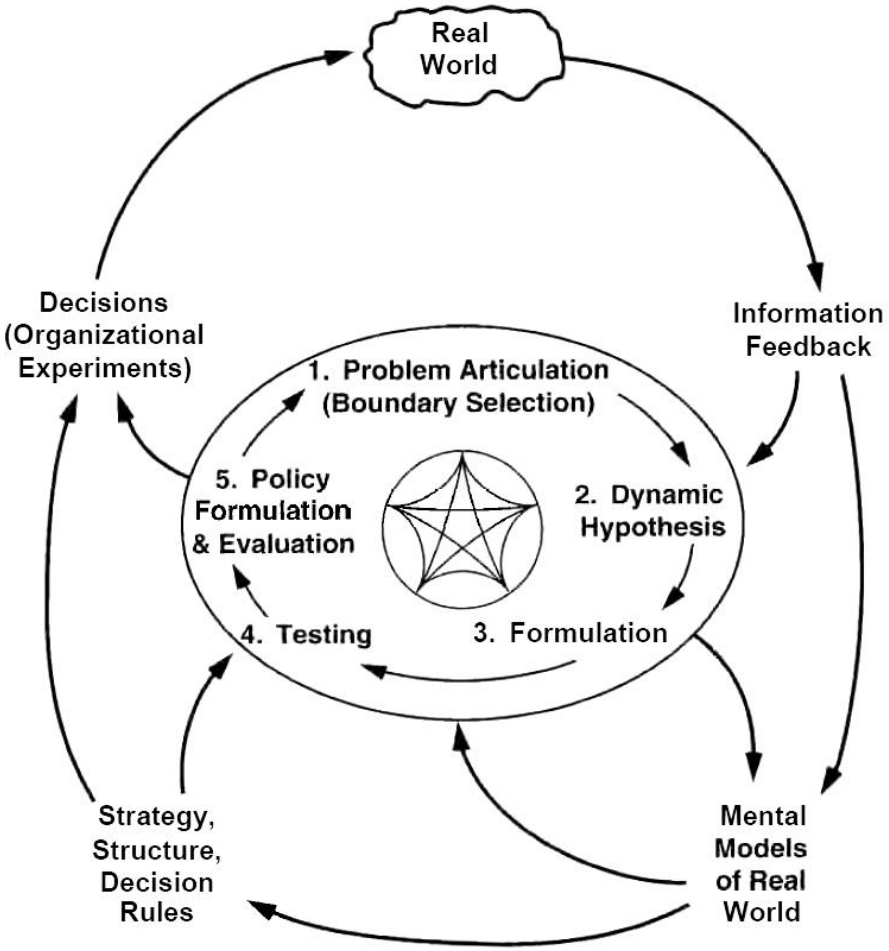
4) **Zlepšení mentálních modelů**

Bureš [5] popsal jednotlivé kroky systémové analýzy a syntézy v 7 krocích:

1. **Analýza problémové oblasti**
2. **Formulace problémů**
3. **Formulace cílů řešení**
4. **Definování a identifikace systému**
5. **Analýza a syntéza systému**
6. **Interpretace a komunikace řešení**
7. **Implementace a realizace řešení**

Nejucelenější postup, včetně znázornění diagramem, přestavil Sterman [11]**:**

1. **Vyjádření problému**
   a) výběr tématu
   b) klíčové proměnné
   c) časový horizont
2. **Formulace dynamické hypotézy**
   a) výchozí vytvoření hypotézy
   b) průzkum endogenních vlivů
   c) mapování systému pomocí diagramů
3. **Sestavení simulačního modelu**
   a) Specifikace struktury
   b) určení parametrů, chování a úvodních podmínek
4. **Testování**
   a) porovnávání s referenčním módem
   b) robustnost za extrémních podmínek
   c) citlivost
5. **Návrh postupu a hodnocení**
   a) specifikace postupů
   b) návrh scénářů



Obr. 8: Modelování systému jako dynamický iterativní proces se zpětnými vazbami
Zdroj: převzato z [11]

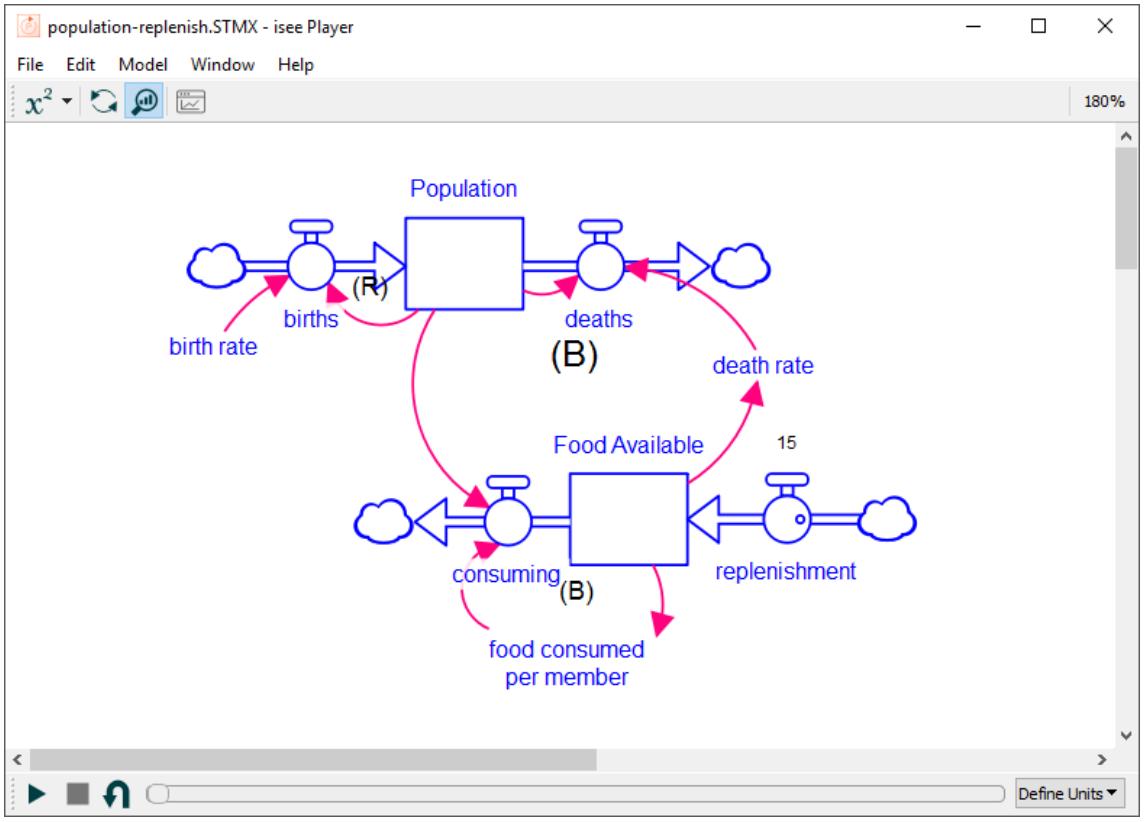
3.6 Použité modelovací a simulační softwarové nástroje

„Nástroje pro počítačovou simulaci systémové dynamiky dovolují vytvářet mikrosvěty, kde prostor a čas mohou být smrštěny a zpomaleny, čímž umožňují poznat dlouhodobé následky a vývoj a rozvíjet naše porozumění komplexních systémů a následně navrhovat struktury a strategie vedoucí k většímu úspěchu [11]“.

Jak bylo již výše zmíněno, první nástroj pro počítačovou simulaci systémové dynamiky, *SIMPLE*, byl vytvořen pro Forresterovy účely programátorem Richardem Bennettem. Jack Pugh poté software rozšířil do podoby simulačního jazyka *DYNAMO*. V současnosti se nabízí například software *Powersim*, *Vensim*, *NetLogo* a *Stella*, kterou zmiňuje i Forrester [18] v souvislosti s její uživatelskou přívětivostí. Výhodou současných modelovacích nástrojů je, že uživatel pracuje s jednoduchým grafickým rozhraním a je odstíněn od matematických výpočtů diferenciálních rovnic, na kterých je fungování programů založené [5].

Pro účely této práce je k modelování systémů použit software *Stella 10.0* z roku 2012. Program je dílem společnosti *isee systems* (původně *High Performance Systems*), kterou v roce 1985 založil Barry Richmond [19].

K vizualizaci a simulaci modelů je použit software *isee Player 1.1.2* z roku 2016, protože nabízí přívětivější uživatelské rozhraní a vyspělejší metody grafického znázornění systémů. Oba programy společnosti *isee systems* bohužel nepodporují českou diakritiku.



Obr. 9: Rozhraní programu *isee Player 1.1.2*
Zdroj: vlastní zpracování

4 Kybernetické hrozby a bezpečnost

4.1 Druhy kybernetických hrozeb

Prozatím patrně nejucelenější přehled kybernetických hrozeb představila ENISA ve své výroční publikaci *ENISA Threat Landscape 2015* [20]. ENISA uvádí, že se snaží přehled udržovat neustále aktuální a že ho během posledního roku adoptovali mnozí hráči v oblasti kybernetické bezpečnosti [21]. ENISA mj. publikuje i přehledy hrozeb pro konkrétní oblasti, např. pro smart grid, IoT, smart nemocnice atd....

Ve zmíněné publikaci se hrozby dělí do 9 hlavních skupin, níže následuje jejich výčet a uvedení několika příkladů ke každé z nich. Přehlednější a podrobnější znázornění je dispozici v příloze 1.

- **neúmyslná (náhodná) poškození**
  nechtěný únik/sdílení informací, neúmyslná změna dat v informačním systému, chyby v návrhu
- **zločinné aktivity/zneužívání**
  neoprávněný přístup, zneužití dat, manipulace s daty a informacemi, spam, hoax, cílené útoky, DoS, badware (vir, červ, botnet, adware …)
- **přírodní a ekologické katastrofy**
  požáry, záplavy, úder blesku, husté sněžení, elektromagnetická bouře, úniky radiace, prach, koroze
- **poškození/ ztráty**
  ztráta/zničení zařízení nebo dat, únik informací, ztráta dat v cloudu, škoda způsobená třetí stranou
- **odposlechy/zachytávání/únos spojení**
  špionáž státní/korporátní, wardriving, odposlechy pomocí HW/SW
- **selhání/poruchy**
  Selhání/poruchy zařízení, dodávek služeb, chyby v softwaru a konfiguraci
- **výpadky/nedostatky**
  výpadek sítě/internetu/elektřiny nebo jiných zdrojů, nepřítomnost/nedostatek personálu, stávka
- **právní hrozby**
  rozhodnutí/nařízení soudu, porušení zákonů nebo regulací

- **fyzické útoky**
  sabotáže, vandalismus, teroristické útoky, válečné poškození

Co se týče špionáže (ať už z důvodů ekonomických, vojenským, politických nebo jiných), hrozbu představují obě myslitelné možnosti, tedy že stát/podnik je cílem špionáže, ale i „orwellovská" varianta, že podnik nebo stát (resp. jeho bezpečnostní složky) špionáž provádí, a jak upozorňuje NBÚ [22] a aféry z posledních let, je tato možnost stále častější a obecně vzestup kybernetické špionáže a státem sponzorovaných aktivit podle [1] představuje novou hrozbu Evropské státy a společnosti.
Nutno podotknout, že kvůli dělení hrozeb podle původu a snaze je co nejvíc rozčlenit se v přehledu ztrácí část hrozeb vzniklých kombinací několika dílčích nebo přesahujících do jiných oborů. Podle NBÚ [22] a agentury ENISA [21] riziko představuje například cenzura internetu, na vzestupu je také mj. působení organizovaného zločinu v kyberprostoru, hacktivismus, záměrné šíření dezinformací a ohýbání reality za účelem dosažení politických a vojenských cílů. Pozornost se upíná i na kyberterorismus, ke kterému zatím nebyla přiřazena žádná konkrétní hrozba, ale do budoucna se s ním počítá.

4.2 Kybernetické hrozby pro ČR

Bezpečností strategie České republiky z roku 2015 [23] identifikovala mezi bezpečnostními hrozbami pouze kybernetické útoky. Ve stejném duchu se vyjadřuje i *Bílá kniha o obraně* [24] připravená Ministerstvem obrany. Oproti tomu *Národní strategie kybernetické bezpečnosti pro období let 2015–2020* (zkráceně *NSKB*) [22] už naštěstí takovým zjednodušením netrpí. Představuje mnoho hrozeb obecnějších i naprosto specifických. Obecnější hrozby zahrnují: mobilní malware, big data a cloud (pro jeho netransparentnost), používání sociálních sítí, přechod z IPv4 na IPv6, zabudování a zneužití zadních vrátek v hardwaru.

Specifičtější hrozby ve vztahu k ČR byly v *NSKB* identifikovány následující:

- **ČR jako možný testovací objekt**
  ČR používá ke svému zabezpečení podobné technologie, mechanismy a procesy jako další státy a hrozí, že poslouží útočníkům k otestování útoku na významnější státy. Před hrozbou útoků a boje v kyberprostoru varují i Balabán, Pernica a kolektiv [25] a varují také před dezinformačními kampaněmi k ovlivňování veřejného mínění, kterými jsou současné konflikty doprovázené.

- **Nedostatečná důvěra veřejnosti ve stát**

  Bezpečnost nebude fungovat bez dobrovolné spolupráce všech občanů, soukromého sektoru (pod který patří většina kyberprostoru [22]) a organizací zajišťujících kybernetickou bezpečnost.
- **Hrozby spojené s digitalizací veřejné správy (tzv. eGovernment)**

  V *NSKB* jsou zmíněna bezpečnostní rizika. Prof. Král [26] má méně všední úhel pohledu: Rozvoj ICT podporuje růst složitosti administrativních procesů a státní správa se i přes velké investice do eGovernmentu nijak nezjednodušuje, naopak má prostor k růstu, což je hrozba pro budoucí vývoj společnosti. Jako historickou paralelu uvádí úpadek Osmanské říše, ke kterému údajně přispělo osvojení výroby papíru a tím způsobený enormní nárůst byrokracie.
- **Ochrana průmyslových řídicích systémů a informačních systémů ve zdravotnictví**
- **Narůstající závislost obranných složek na ICT**

  Ohroženy jsou systémy, sítě i samotná technika (vozidla, letadla, …), což ohrožuje obranu státu a provádění vojenských akcí. Obranné složky musí umět na kybernetické hrozby reagovat a zneškodnit je.
- **Nízká digitální gramotnost koncových uživatelů**

  Základní povědomí o možných hrozbách chybí uživatelům z řad veřejnosti i státní správy.
- **Hrozby spojené s internetem věcí (IoT) a inteligentními energetickými sítěmi (Smart Grid)**

  Digitalizace dříve pasivních systémů přináší nové možnosti zneužití, počet zařízení připojených k internetu neustále narůstá a jejich zabezpečení je často mizerné, jak upozorňuje i Ministerstvo vnitra [27]. To je ještě umocněno negramotností uživatelů.
- **Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství**

  Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti neodpovídá aktuálním požadavkům a trendům. Nedostatečně vzdělává a vychovává žáky na základním a středním stupni a také v nedostatečné míře nabízí vysokoškolské programy produkující odborníky na kybernetickou bezpečnost. Poptávka po nich je přitom vysoká.

- **Nedostatečné zabezpečení malých a středních podniků**

  Malé a střední podniky si neuvědomují svůj význam a potřebu zabývat se kybernetickou bezpečností, nemají odpovídající prostředky ani znalosti, přestože mohou pracovat s kritickými daty nebo systémy.

  Z šetření ČSÚ z roku 2016 [28], které nově zahrnovalo i bezpečnost a ochranu dat vyplývá, že bezpečnost neřeší průměrně 20,5 % podniků, konkrétně 23,2 % podniků s 10–49 zaměstnanci, 10,8 % s 50–249 zaměstnanci a 7,6 % s 250 a více zaměstnanci. Z jiného šetření vyplynulo [29], že pouze 33,4 % podniků má definovanou bezpečnostní politiku informačního systému, nejhůře jsou na tom opět malé a střední podniky.
- **Rostoucí počet uživatelů internetu a ICT a z toho plynoucí kritičnost jejich selhání**

  Podle ČSÚ [30] byl v Česku v roce 2015 podíl elektronických tržeb na úrovni 31 %, tzn. 3. nejvyšší v EU, v témže roce elektronicky nakupovalo 62,3 % podniků, ještě v roce 2005 to bylo pouhých 27,9 %. S rostoucí závislostí veřejné a soukromé sféry na internetu a ICT roste i kritičnost jejich selhání, především u systémů podle zákona spadajících mezi kritickou informační infrastrukturu (KII) nebo významné informační systémy (VIS).
- **Rostoucí kyberkriminalita a kybernetické útoky**

  Rozvoj kyberkriminality souvisí s povahou kyberprostoru a se všemi výše uvedenými hrozbami, proto byla v této práci kyberkriminalita vyčleněna do samostatné podkapitoly a zvýšená pozornost je jí věnována i při modelování systému.

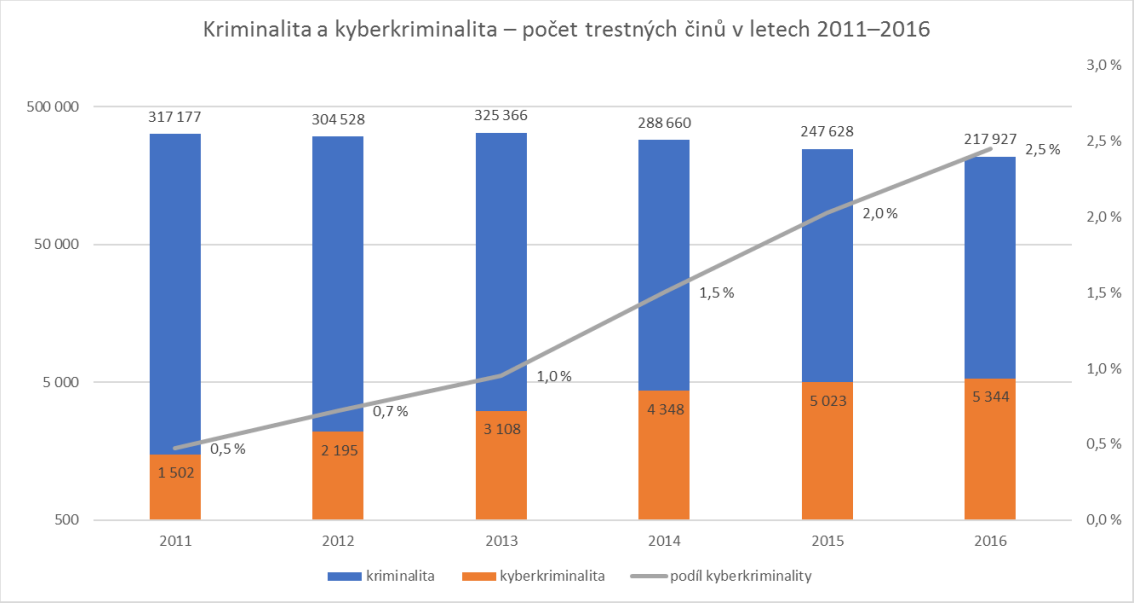
4.2.1 Kyberkriminalita

Policie ČR [31] vymezuje kyberkriminalitu (lze se ve stejném významu setkat i s pojmem informační kriminalita) jako trestnou činnost, která *„je páchána v prostředí informačních a komunikačních technologií, kdy předmětem útoku je buď samotná oblast informačních a komunikačních technologií, případně je tato trestná činnost prováděna za výrazného využití informačních a komunikačních technologií*.“

Podle *NSKB* [22] rostou možnosti obchodování s citlivými informacemi, charakter internetu pachatelům dává možnosti provádět cílené i masové útoky a slibuje rychlý účinek a zisk a současně nízké riziko postihu. Zpráva Ministerstva vnitra [27] popisuje nárůst informační kriminality – ze všech forem kriminality roste nejrychleji už mnoho let v česku i zbytku světa a vzhledem k růstu role ICT nelze očekávat změnu. V ČR bylo za rok 2016 zjištěno 5344 případů kyberkriminality a počet případů každoročně roste. Bohužel, v této oblasti je

typická mimořádně vysoká míra latence, jak zdůrazňuje i [25] a [32], takže většina případů zůstane nezjištěna nebo nenahlášena, nejen kvůli obtížné odhalitelnosti, ale i vysoké míře tolerance nebo lhostejnosti ze strany společnosti. Celkové množství incidentů, automatizovaných i cílených útoků, úspěšných i neúspěšných, odhadovalo Ministerstvo vnitra v roce 2014 na přibližně 200 tisíc incidentů denně.

ENISA [21] upozorňuje, že trendem roku 2016 bylo zpeněžení kyberkriminality, útoky jsou stále důmyslnější a optimalizovanější na zisk. Podle údajů Police ČR [31] a Ministerstva vnitra [27] se struktura zaznamenávané trestné činnosti v ČR téměř nemění, nejčastěji jde o podvodná jednání, o porušování autorských práv, různé podvodná jednání, s velkým odstupem pak o krádeže elektronických dat, útoky zaměřené na destabilizaci datových sítí, šíření závadného elektronického obsahu (dětská pornografie, extremistická ideologie), ale také o vydírání, vyhrožování, porušování tajemství dopravovaných zpráv, padělání veřejných listin a poměrně nově i o tzv. stalking (nebezpečné pronásledování) a kyberšikanu. Objevují se také činy související s drogovou oblastí a ostatní trestnou činností. Policie ČR často řeší ochranu seniorů a dětí na internetu, daří se jí např. pravidelně narušovat struktury zodpovědné za šíření dětské pornografie.



Obr. 10: Vývoj kriminality a kyberkriminality
Zdroj: vlastní zpracování podle dat Policie ČR [31] a ČSÚ [33]

Kromě obtížné odhalitelnosti patří kyberkriminalita mezi vůbec nejproblematičtější z hlediska určení místní příslušnosti. Roli zde hraje např. umístění serverů, poskytovatelů služeb, síťových uzlů atp.…
Rozvoj technik kyberkriminality rychle roste, probíhá profesionalizace pachatelů informační kriminality, která vykazuje stále větší míru propracovanosti s jasnější dělbou jednotlivých rolí, pachatelé se stále častěji snaží zakrýt své jednání pomocí kryptovacích mechanizmů, často také používají botnetové sítě, které přispívají k anonymitě, masivnosti a technologické koordinaci útoku.

V současnosti ne všechny státy EU mají potřebné prostředky a schopnosti na účinný boj s kyberzločinem [1]. Europol uvádí [34], že kyberzločiny ročně stojí státy EU 256 miliard eur, celosvětově pak 900 miliard eur.

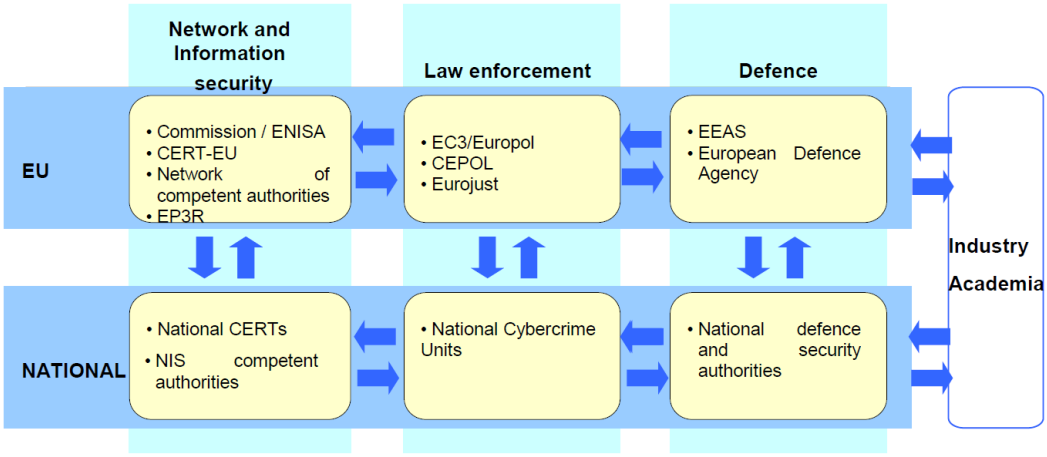
4.3 Kybernetická bezpečnost

Kybernetická strategie EU [1] obsahuje definici: „*Kybernetická bezpečnost běžně odkazuje na bezpečnostní prvky a akce sloužící k ochraně civilního i vojenského kyberprostoru před hrozbami souvisejícími nebo narušujícími sítě a informační infrastrukturu. Kybernetická bezpečnost usiluje o zachování dostupnosti a integrity sítí a infrastrukturu a důvěrnosti obsažených informací.“*

Kvůli narůstající sofistikovanosti a ničivosti kybernetických útoků a dalších hrozeb NATO uznalo v roce 2016 kyberprostor jako 5. bojiště [35], chce na něm podnikat zejména obranné operace v souladu s mezinárodním právem. Pro zajištění obrany kyberprostoru chce spolupracovat s průmyslem, zlepšit bezpečnost a sdílení informací a osvědčených postupů mezi členskými zeměmi [36].

Bílá kniha o obraně [24] i *Bezpečností strategie EU* [37] v souvislosti nejen s kybernetickými hrozbami pokazují na stírání rozdílů mezi vnitřní a vnější bezpečností státu. Kybernetická bezpečnost v podání EU [1] zahrnuje posílení technologických kapacit na zmírnění hrozeb a zvýšení odolnosti kritické infrastruktury, sítí a služeb a omezení kyberkriminality. EU vidí prioritu v posílení součinnosti civilního a vojenského přístupu ke kybernetické bezpečnosti. Tyto snahy by měly být podporovány výzkumem a vývojem, užší spolupráci mezi vládami, soukromým sektorem a akademickou sférou EU.
Komplexní kybernetická bezpečnost na celoevropské úrovni by měla stát na třech pilířích, vymezených právními rámci: bezpečnost sítí a informací, vymáhání práva a obrana.

Odpovídající organizace by pak měly náležitě spolupracovat v případech jako kybernetická špionáž, státem sponzorovaný útok nebo jiný závažný incident s celonárodními důsledky. V takových případech by také měl být použit mechanismus včasného varování a krizové řízení nebo další procedury. Částečnou implementaci takových mechanismů zahrnuje i *NSKB*.



Obr. 11: Tři pilíře kybernetické bezpečnosti v EU a vazby mezi nimi
Zdroj: [1]

U národních a nadnárodních organizací zaměřených na kybernetickou bezpečnost také upozorňuje na potřebu vyhnut se nechtěné duplikaci rolí a funkcí těchto organizací, prioritou bude jasné vymezení rolí, zodpovědností a právních opatření. Výše zmíněná strategie EU připomíná, že stále existují mezery, a to hlavně v oblasti národních kapacit, spolupráce v případě incidentů přesahujících hranice a v oblasti zájmu a připravenosti soukromého sektoru. Soukromému sektoru také chybí motivace k poskytování spolehlivých údajů o výskytu a dopadu bezpečnostních incidentů příslušné autoritě (tj. národnímu CERT týmu v případě ČR), implementaci vyhodnocování rizik a investice do bezpečnosti. Navrhovaná legislativa se proto na tyto aspekty zaměří, a to především u veřejné správy, poskytovatelů internetového připojení, energie, dopravy, v bankovnictví a burzách.

V dokumentu je dále zdůrazněno, že vyšší úrovně zabezpečení může být dosaženo pouze v případě, kdy všichni v hodnotovém řetězci (výrobci vybavení, SW vývojáři, poskytovatelé služeb) budou považovat bezpečnost za prioritu. Avšak zdá se, že bezpečnost stále představuje jen zátěž navíc a poptávka po ni je omezená. Podle EU centralizované řešení nemá smysl, lepší je přístup na národní úrovni, jednotlivé vlády mohou lépe čelit incidentům a spolupracovat se soukromým sektorem. Účinná státní odezva na hrozby přesto bude znamenat celoevropské úsilí.

4.3.1 Soukromý sektor

Protože většina kyberprostoru je vlastněna soukromým sektorem, je důležité sledovat vývoj i v této oblasti. Pozornost se upíná na analýzu bezpečnostních incidentů, probíhá vývoj metod a metodik hodnocení, situace v mnoha organizacích zůstává neutěšená. Odrazující jsou především náklady na analýzu. ENISA podotýká [20], že ke správnému rozhodování bude potřeba obrovské množství dat z vyhodnocených incidentů a jejich výsledků.

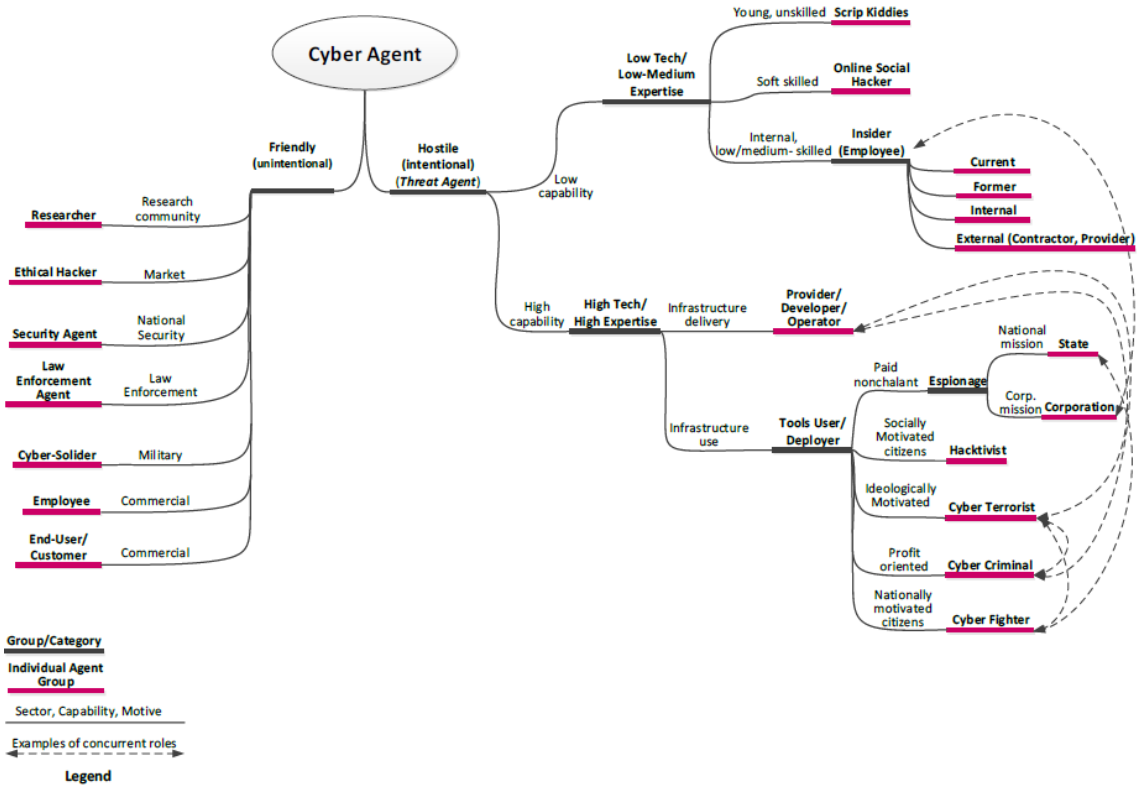
Podle McAfee [38] v bezpečnostní průmyslu v současné době probíhá vývoj standardů a osvědčených postupů pro sdílení informací a analýzu. Podniků a služeb, komerčních i neziskových, totiž působí na poli kybernetické bezpečnosti mnoho, jednota v přístupu a poskytovaných službách a řešeních zatím chybí. Zatím je běžné, že společnosti o incidentech zaznamenávají a sdílí různé údaje, byť se jedná o stejnou hrozbu. Překážkou při implementaci sdílení informací se ukazuje nutnost vyhnout se sdílení důvěrných dat z oblasti působení společnosti, a to z důvodů vnitřních zásad organizace i zákonem omezených způsobů nakládaní s daty zákazníků nebo pacientů. Dalšími překážkami jsou podceňování hrozeb managementem organizací (kvůli nedostatečné informovanosti), nepochopení přínosu analýzy a sdílení (přestože na jeho potřebě se podniky shodují) a již zmíněné finanční náklady.

4.3.2 Kyber agenti

Jednotlivci interagující s kyberprostorem jsou v odborných zdrojích označováni pojmem *kyber agenti*. ENISA [20] je dělí na *přátelské*, kteří hrozbám čelí, a *nepřátelské (Threat Agent)*, původce hrozeb. Původci se zatím zdají vždy být o krok napřed, nahrává jim i asymetrie obrany a útoku [39], tedy skutečnost, že útočníkům stačí najím 1 slabinu, kdežto obránci potřebují najít a zabezpečit všechny.

Do skupiny čelící hrozbám patří výzkumníci, pracovníci bezpečnostních agentur, etiční hackeři, organizace na prosazování zákona, kybervojáci, zaměstnanci firem a koncoví uživatelé nebo zákazníci. Výhledově se počítá také se zapojením schopných dobrovolníků z řad odborné veřejnosti, pracujících pro dobré zájmy na vlastní zodpovědnost.

Mezi původce hrozeb patří státy, podniky, kyberteroristé a bojovníci, kyberzločinci, tzv. insideři – zaměstnanci firem (bývalí i současní, externí i interní), hackeři, poskytovatelé služeb.



Obr. 12: Přehled kyber agentů jako součást proaktivního přístupu k bezpečnosti
Zdroj: převzato z [20]

4.3.2.1 Původci hrozeb

V oblasti hrozeb a incidentů záměrně zapříčiněných lidskou činností panuje stále řada nejasností. Výzkumy se snaží zjistit více o původcích hrozeb, cílem je zjistit více o jejich motivaci, způsobu práce a případné vzájemné výměny informací.

Podle agentury ENISA [20] lze zevrubné znalosti o původcích hrozeb a (přístup k získání takových znalostí) rozdělit do tří skupin:

Obr. 13: Rozdělení znalostí o původcích hrozeb
Zdroj: převzato z [20]

Proaktivní znalosti jsou takové, které mohou být známy ještě před výskytem incidentu. Například skupiny původců, dovednosti, motivace, interakce a vztahy mezi skupinami. Takové znalosti mohou být použity při analýze rizik, ale volně dostupných informací tohoto druhu byl v roce 2015 nedostatek a bylo konstatováno, že oblast potřebuje detailněji prozkoumat.

Realtimové znalosti představují informace o současném dění, které poskytují média a online zdroje. Cenné informace jsou často nepřístupné, přestože by byly nápomocné nejen v analýze rizik, ale i plánování konkrétních akcí.

Reaktivní znalosti („*ex post*“) jsou výsledkem analýzy úspěšně rozpoznaných incidentů. Umožnují porozumět metodám útoku, jeho autorům a motivacím. Tyto znalosti mají po analýze incidentů k dispozici organizace na prosazování zákona, bezpečností agentury a podobné organizace.

Proběhly výzkumy motivace, uvažování a pozadí agentů. Společnost Intel v roce 2015 zahrnula motivaci do svých přehledů hrozeb [40]. Druhy motivace zahrnují: náhodnost, donucení, nespokojenost, snahy o dominanci, ideologie, snahu o uznání druhých, prospěch pro organizaci, finanční prospěch, osobní uspokojení, nepředvídatelnost. Z kombinací více motivací bylo definováno 18 druhů agentů (ukázka v příloze 2).

Proběhly také analýzy online diskuzních fór, chatovacích místností a obchodů osvětlující chování agentů. K identifikaci útočníků pomohla také analýza běžných anonymizačních metod a jejich slabin [21]. Přibyly i informace o hrozbách způsobených zevnitř (zaměstnanci apod.), coby výsledek reaktivní analýzy.

Jak dodává McAfee [38], přestože tyto znalosti jsou cenné, stojíme teprve na počátku skutečného porozumění životního cyklu hrozeb.

4.4 Kybernetická bezpečnost ČR

NSKB [22] nabízí poměrně komplexní definici kybernetické bezpečnosti ČR: „*Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.*“

Balabán, Pernica a kolektiv [25] považují kybernetickou bezpečnost ČR za otázku bytí a nebytí moderní civilizace a zdůrazňují, že největším problémem je v současnosti

nedostatečné personální, materiální a organizační vybavení příslušných pracovišť. Specializované policejní kapacity jsou podle nich plně vytíženy běžnou agendou a postrádají rezervy, které by jim umožnily sledovat aktuální trendy nebo provádět aktivní operace v kyberprostoru. Obdobná situace panuje i v rámci zpravodajských služeb.

Dále Balabán a Pernica upozorňují na problém, kdy dosažené úspěchy nejsou odpovídajícím způsobem prezentovány v mediích a na opačný jev (pozorovaný ve státní bezpečnosti i politice), tzv. *media-driven security policy*, tedy jednání, které místo konání akcí více dbá na vytvoření dojmu a uspokojení mediální poptávky.

Kroky ČR v této oblasti probíhají podle Balabána a Pernici hektickým tempem, stát dohání několikaletý skluz způsobený kompetenčními spory po zániku Ministerstva informatiky, které působilo mezi lety 2003–2007. Změna nastala až roku 2011, kdy vláda ČR tímto úkolem pověřila Národní bezpečnostní úřad. NBÚ připravil *Národní strategii kybernetické bezpečnosti* na období 2012–15 a na období 2015–20 a na ně navazující Akční plány. ČR také spolupracuje s agenturou ENISA a pravidelně se účastní mezinárodních cvičení kybernetické bezpečnosti, Ministerstvo obrany i NBÚ se aktivně se účastní projektů a cvičení NATO v této oblasti, snaží se plnit požadavky EU a NATO (implementace a plnění právních a jiných předpisů a požadavků). NBÚ postupně navazuje spolupráce s dalšími zahraničními partnery a v rámci ČR se snaží o osvětu v oblasti kybernetické bezpečnosti formou přednášek, školení a spolupráce s některými vysokými školami [27].

Současnou situaci shrnuje v *NSKB* [22] Ing. Dušan Navrátil tak, že předešlá strategie na roky 2012–15 byla zdárně realizována a došlo ke znatelnému navýšení kybernetické bezpečnosti. Podotýká, že „*kybernetické bezpečnosti však nelze dosáhnout bez hluboké důvěry a spolupráce mezi veřejným sektorem a zbytkem společnosti*“ a že žádný veřejný či soukromý subjekt, ani jednotlivec v ČR se nesmí zříci své zodpovědnosti a role při zajišťování kybernetické bezpečnosti.

4.4.1 Legislativa

Zpracováno podle zdrojů: [27] [41] [42]. 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti, publikovaný ve sbírce zákonů od srpna 2014. Vychází z norem řady ISO/IEC 27k. Během roku 2017 by měla proběhnout jeho novelizace za účelem odstranění nedostatků zjištěných během dvou let účinnosti zákona, a především nutnosti implementace evropské směrnice NIS (č. 2016/1148).

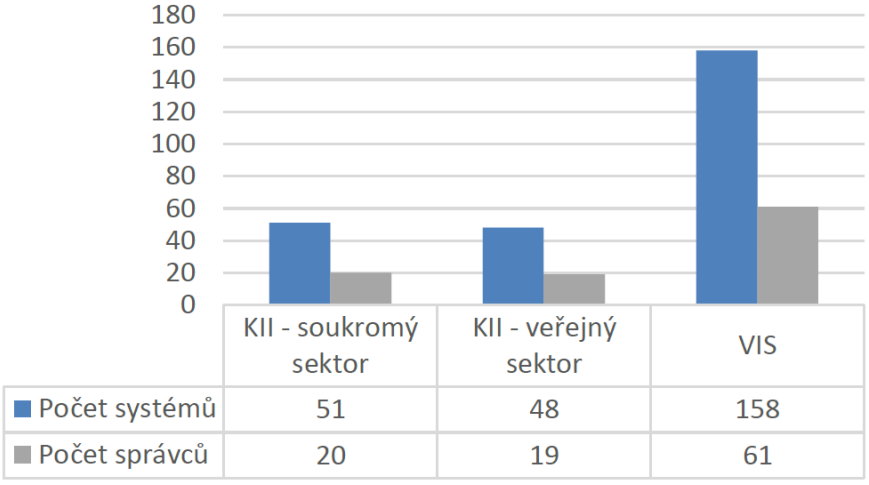
Směrnice NIS stanovuje základní kritéria pro přístup členských států ke kybernetické bezpečnosti, aby došlo ke sjednocení a vyrovnání situace. K subjektům definovaným v zákoně o kybernetické bezpečnosti přidává dvě nové obecné kategorie – provozovatele

základních služeb a poskytovatele digitálních služeb, kteří budou povinni zavést bezpečnostní opatření a hlásit bezpečnostní incidenty ohrožující kontinuitu poskytování jejich služeb a jimi zajišťované společenské a ekonomické aktivity. Směrnice zřizuje dvě nové platformy pro spolupráci členských států EU, a to Skupinu pro spolupráci pro strategické otázky a Síť CSIRT týmů pro technickou spolupráci. Další požadavky stanovené směrnicí už nejsou pro ČR stěžejní, byly vyřešeny už dříve přijetím zákona o kybernetické bezpečnosti.

Se zákonem o kybernetické bezpečnosti souvisí následující právní předpisy:

- Vyhláška č. 316/2014 Sb., která stanovila bezpečnostní opatření, typy a kategorie bezpečnostních incidentů, reaktivní opatření a náležitosti hlášení a komunikace v oblasti kybernetické bezpečnosti a dále požadavky na dokumentaci kritické infrastruktury a informačních systémů.
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Kvůli pokračující identifikací nových systémů byla v roce 2016 novelizována.
- Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvků kritické infrastruktury, která bylo novelizováno s přijetím zákona o kybernetické bezpečnosti.

Legislativa v rámci ČR vymezuje *kritickou informační infrastrukturu (KII)* a *významné informační systémy (VIS)* a stanuje povinnosti pro jejich provozovatele a správce. Kategorizaci systémů provádí NBÚ ve spolupráci s dotyčnými subjekty, jedná s nimi o dalších opatřeních a provádí kontroly.



Obr. 14: Počty systémů KII a VIS v roce 2016
Zdroj: převzato z [43]

4.4.2 Vzdělávání a osvěta

„Míra povědomí většiny populace o nebezpečích souvisejících s užíváním informačních a komunikačních technologií nicméně zůstává značně neuspokojivá. Zdaleka ne všechny osvětové či vzdělávací aktivity v minulosti naplnily očekávání do nich vkládaná (jednalo se o akce jednorázové, teritoriálně omezené či nepřizpůsobené konkrétnímu publiku) [25]."

Mimoškolní osvětové aktivity se soustředí na odbornou veřejnost, především na IT specialisty a správce sítí. Na co možná nejširší publikum na celorepublikové úrovni byl zacílen seriál *Jak na internet*, který realizovalo v letech 2012–2014 sdružení CZ.NIC, včetně doprovodných výukových materiálů [44]. Na užší skupinu diváků se zaměřil navazující seriál *Nebojte se Internetu.* Oba seriály odvysílala Česká televize (druhý jmenovaný pod názvem *Internet pro seniory*).

4.4.2.1 Školství

Národní strategie kybernetické bezpečnosti na roky 2015–2020 [22] uvádí jako hrozbu nedostatek odborníků na kybernetickou bezpečnost a potřebu úprav současných studijních plánů ve školství. Je konstatováno, že vzdělávání v této oblasti na základních, středních ani vysokých školách v Česku neodpovídá potřebám a trendům současné doby. Odborníci jsou nedostatkovým zbožím. Prof. Král [26] zmiňuje také absenci některých profesí a vzhledem k rychlému vývoji ICT i nutnost celoživotního vzdělávání, na kterém by měly spolupracovat všechny instituce, které ve vzdělávání působí. Zmiňuje také potřebu IT odborníků ovládajících znalosti i z humanitních a jiných oborů.
NBÚ [45] ve spolupráci s Ministerstvem školství, Ministerstvem práce a sociálních věcí a odborníky z veřejné správy, neziskového a komerčního sektoru v roce 2015 vypracoval *Návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti*.

Základní a střední školy jsou mnohdy v zoufalé situaci ve využívání ICT obecně, což je způsobeno nedostatečnými financemi a již zmiňovaným nedostatkem lidí disponujících potřebnými a aktuálními znalostmi. Tomu odpovídá stav výuky v této oblasti, forma využívání ICT při běžné výuce i samotná bezpečnost školních systémů a dat [46]. Snaze pomoci vyučujícím je věnováno úsilí v několika neziskových projektech.
Situaci na vysokých školách v roce 2015 zkoumal i NBÚ, provedl mapování vysokoškolských programů, oborů a předmětů zaměřených nebo souvisejících s kybernetickou bezpečností. Zahrnuty byly technické i humanitní směry, celkem bylo osloveno 38 vysokých škol.

Dostupná evidence pravděpodobně není kompletní, např. nezahrnuje předměty vyučované na FIM UHK a skutečný počet univerzit a předmětů může být větší.
Z výsledků mapování vyplývá [47], že na veřejných vysokých školách se často jedná jen o jednotlivosti nebo konkrétní metody zabezpečení v rámci výuky počítačových sítí, operačních systémů, kryptografie a kryptologie, práva. Soukromé školy se věnují podobným tématům převážně z manažerského hlediska. Předměty na státních školách, Univerzitě obrany a Policejní akademii ČR, kromě výše zmíněných předmětů zkoumají problematiku s větším nadhledem, a to včetně bezpečnostně-politického a vojenského hlediska.
NBÚ [45] uzavřel smlouvy o spolupráci s Vysokou školou báňskou, Univerzitou Tomáše Bati, Jihočeskou univerzitou a Karlovou univerzitou, jeho zástupci přednášeli na Palackého a Masarykově univerzitě a údajně plánují spolupráci i s dalšími školami.

4.5 Organizace zabývající se kybernetickou bezpečností

4.5.1 Na mezistátní úrovni se vztahem k ČR

Nato [27] [43]
Nato v roce 2016 uznalo kyberprostor jako 5. operační doménu a potvrdilo, že i kybernetická obrana je součástí kolektivní obrany. S NATO v této oblasti spolupracuje NBÚ a Ministerstvo obrany (přesněji Vojenské zpravodajství a Národní centrum kybernetických sil) a společně se podílejí na výzkumných a vědeckých projektech a pravidelně se účastní aliančních cvičení Locked Shields a Cyber Coalition, které testuje připravenost států NATO na kybernetické útoky, hlavně schopnost efektivního rozhodování při zvládání kybernetických krizí a schopnosti států vyměňovat relevantní informace pro jejich řešení, nebo potřebné technické a právní kapacity.
V roce 2016 přijat Cyber Defence Pledge, na jehož tvorbě se podílelo i české NCKB. Státy se v dokumentu zavázaly budovat a posilovat bezpečnost národních sítí a informační infrastruktury a navýšit odolnost proti kybernetickým útokům. Proto byla schválena i metrika, pomocí které se bude posuzovat navyšování kybernetických schopností členských států.

OBSE [43] [48]
OBSE řeší rozmanité kybernetické hrozby včetně kyberkriminality a zneužívání internetu pro teroristické účely. Zaměřuje se především na posilování vzájemné důvěry členských států a omezení rizika konfliktu vzešlého z užívání ICT. Pro ČR, reprezentovanou NBÚ a

Ministerstvem zahraničních věcí, je OBSE užitečným zdrojem informací o postojích a politikách v oblasti kybernetické bezpečnosti uplatňovaných ve státech mimo EU či NATO.

4.5.2 Na úrovni EU

European Cybercrime Centre (EC3) v rámci Europolu [34]

Přístup EC3 k boji s kyberkriminalitou se skládá ze tří prvků: strategie zahrnující osvětu, podporu tréningu a budování kapacit, dále z pokročilé forenzní analýzy a vlastních akcí a operací. EC3 se soustředí především na organizovaný zločin v kyberprostoru, kybernetické útoky na kritickou informační infrastrukturu a informační systémy a na vážně poškozené oběti, např. online dětské pohlavní zneužívání.

European Union Agency for Network and Information Security (ENISA) [49] [45]

Agentura Evropské unie pro bezpečnost sítí a informací byla zřízena v roce 2004. V roce 2016 měla 65 zaměstnanců, z toho 3 byli zástupci českého NBÚ. Shromažďuje odborné poznatky v zájmu kybernetické bezpečnosti v Evropě, poskytuje poradenství a řešení pro veřejný a soukromý sektor v zemích EU i pro orgány EU, spolupracuje s Evropskou komisí a členskými státy EU při vývoji národních strategií kybernetické bezpečnosti, koordinuje opatření vydávaná pro zabezpečení jejich sítí a informačních systémů a prostřednictvím kurzů a školení podporuje spolupráci a budování kapacit CERT v jednotlivých členských státech a pořádá celoevropské nácviky řešení krizových situací. Výzkum provádí v úzké spolupráci s Europolem a Evropským centrem pro boj proti kyberkriminalitě, Evropskou agenturou pro bezpečnost letectví (EASA) a dalšími organizacemi.

Central European Cyber Security Platform (CECSP) [45] [50] [51]

Platforma byla založena v roce 2013 na základně iniciativy Rakouska a ČR, jejími členy jsou ČR, Slovensko, Maďarsko, Polsko a Rakousko, 1. setkání proběhlo v Praze. Platforma má vhodně doplňovat jiné evropské nebo mezinárodní organizace, cílem je především sdílení know-how a osvědčených postupů, společná cvičení a vzdělávání. Setkání se účastní zástupci vládních, národních a vojenských CSIRT týmů, bezpečnostních úřadů a center kybernetické bezpečnosti. Byly projednávány možnosti vytvoření zabezpečených informačních kanálů pro omezení úniku informací a podpoře rychlých reakcí.

4.5.3 Na úrovni ČR

Národní bezpečnostní úřad (NBÚ) [45] [52] [43]

NBÚ v rámci ČR zastřešuje oblast ochrany informací, bezpečnostní způsobilosti a kybernetické bezpečnosti. Jeho součástí je Národní centrum kybernetické bezpečnosti (NCKB) a pod něj spadající vládní CERT tým govCERT.CZ. Centrum by se mělo v roce 2017 osamostatnit a zformovat Národního úřad pro kybernetickou a informační bezpečnost a do roku 2025 navýšit personál na 300–400 zaměstnanců. NBÚ, resp. NCKB se v rámci ČR, EU i NATO podílí na přípravě legislativních a jiných významných dokumentů v oblasti kybernetické bezpečnosti.

Národní centrum kybernetické bezpečnosti (NCKB)

NCKB se skládá ze dvou oddělení:

1) Odbor kybernetických bezpečnostních politik (OKBP)

Odbor se zabývá kybernetickou bezpečností z netechnického hlediska. Řeší tvorbu a implementaci kybernetické bezpečnostní politiky ČR. Podle zákona o kybernetické bezpečnosti a dalších předpisů určuje a posuzuje kritickou informační infrastrukturu (KII) a významné informační systémů (VIS). Zabývá se mezinárodní spoluprací, vzděláváním, osvětou a publikační činnost. V roce 2016 bylo nově zřízeno oddělení strategických informací a analýz.

2) Vládní CERT tým GovCERT.CZ

GovCERT.CZ je vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty, pomáhá s jejich řešením, provádí penetrační analýzu, analyzuje malware a sdílí informací o incidentech a aktuálním dění s dalšími týmy, odborníky i veřejností. Záměrem je úzká spolupráce s národním CERT týmem a zastřešování a podpora vzniku dalších české týmů CERT/CSIRT zejména v rámci KII. Od roku 2015 probíhá budování tzv. ICS-SCADA laboratoře pro forenzní analýzu hrozeb, která bude sloužit také při cvičeních kybernetické bezpečnosti a při spolupráci s Policií ČR a Evropským centrem pro počítačovou kriminalitu (EC3) např. při vyšetřování závažnějších útoků a kybernetické kriminality. Laboratoř bude kontinuálně vylepšována a přizpůsobována aktuálním potřebám a vývoji oboru. GovCERT.CZ je od roku 2014 akreditovaným členem Trusted Introducer a od roku 2016 členem organizace FIRST.

Národní CERT tým CSIRT.CZ [46] [53]

CSIRT.CZ je provozován sdružením CZ.NIC, z s. p. o. Plní úlohu národního CERT České republiky podle veřejnoprávní smlouvy s NBÚ a zákona o kybernetické bezpečnosti. Tým nemá výkonné pravomoci, což znamená, že při řešení incidentů působí pouze jako koordinátor, který může poskytnout metodickou pomoc při jejich řešení. Přijímá hlášení o bezpečnostních incidentech a vyhodnocuje je, podílí se na koordinaci řešení incidentů, předává hlášené incidenty osobám odpovědným za chod sítě nebo služby. Polem působnosti CSIRT.CZ je celá Česká republika, tzn. všichni uživatelé a všechny sítě provozované v ČR. Plní roli národního PoC (Point of Contact) pro oblast ICT a podporuje vzdělávání a osvěty v oblasti kybernetické bezpečnosti. V rámci ČR spolupracuje s poskytovateli připojení (ISP), poskytovateli obsahu, bankami, školami, státní správou, bezpečnostními složkami a dalšími institucemi. Na jaře 2017 měl tým 10 členů. Od roku 2011 je akreditovaný u Trusted Introducer, od roku 2015 je členem organizace FIRST.

Ministerstvo vnitra [27] [45]

- **Policie ČR a zpravodajské služby**

  Policie ČR na svém webu zřídila on-line formulář pro hlášení kyberkriminality. V letech 2015 a 2016 pracovala na zajištění personálního a materiálního vybavení specializovaného útvaru pro kybernetickou bezpečnost. Zástupci policie se pravidelně účastní cvičení kybernetické bezpečnosti a rozvíjí spolupráci s GovCERT.CZ a zahraničními partnery včetně Europolu.

  Zpravodajské služby se rovněž účastnily cvičení kybernetické bezpečnosti a pracovaly na plnění úkolů, které jim ukládá *Akční plán národní kybernetické bezpečnosti*.

Ministerstvo obrany [45]

MO úzce spolupracuje s NBÚ. V rámci MO působí Rada pro kybernetickou bezpečnost Ministerstva obrany. 1. června 2015 bylo zřízeno oddělení kybernetické bezpečnosti pro zajištění odborného a metodického řízení a koordinaci činností, ke konci roku 2015 mělo 3 zaměstnance z 9 plánovaných. V plánu je zhotovení *Strategie kybernetické bezpečnosti MO* a *Akčního plánu KB MO na období let 2016 až 2020*.

- **Armáda ČR**
- **Vojenské zpravodajství a Národní centrum kybernetických sil**

4.5.4 CSIRT/CERT týmy

Zpracováno podle: [41] [46] [54]. Postupem času se v rámci organizací i států vyvinula potřeba samostatných celků zabývániích se kybernetickou bezpečností, proto jsou zakládány týmy pro reakci na bezpečnostní hrozby a incidenty, které sbírají a analyzují data, koordinují reakce na incidenty a poskytují informace o hrozbách. Každý tým odpovídá za svoje pole působnosti, typicky sít nebo například doménu. Každý tým má svou pozici v neformální hierarchii, týmy jednotlivých organizací zastřešují CSIRT týmy národní a/nebo vládní, které nemají moc výkonnou (možnost odstranit problém přímým zásahem), ale jejichž role je koordinační a vzdělávací

Pro lepší spolupráci týmů a usnadnění vzájemného kontaktování se postupně vytvořily dvě větší organizace na jejich sdružování a podporu rozvoje a důvěry. První organizace na sdružování týmů, příznačně pojmenovaná First, vznikla v roce 1989. V rámci Evropy působí organizace GÉANT a její služba Trusted Introducer. Členství v nich je dnes jedinou cestou, jak nezávisle ověřit práci a fungování týmu. Každý tým řeší podobné problémy sdílení informací zefektivňuje jejich práci (naopak nespolupráce žádnou konkurenční výhodu nepřináší), vznikají projekty na sdílení dat a vývoj open source nástrojů, které mohou týmy upravovat podle svých potřeb. Vzniká také prostředí pro pomoc novým týmům.

První CSIRT v ČR vznikl v roce 2004 v rámci organizace CESNET, do roku 2014 bylo týmů CSIRT/CERT (registrovaných u Trusted Introducer) v ČR pouze 8. V březnu 2017 už celkem 27 (a 1 čekající na schválení), z toho dva z vládních organizací, jeden národní a ostatní komerční nebo akademické. Na nárůstu počtu týmů se podepsaly DDoS útoky z března 2013 a následný vznik projektu FENIX sdružení NIX.CZ. V rámci Evropy má více etablovaných týmů u Trusted Introducer jenom Německo a Francie [55]. Týmy se na mezinárodní úrovni setkávají třikrát ročně a na úrovni ČR minimálně dvakrát ročně v rámci Pracovní skupiny.

Zákon o kybernetické bezpečnosti definuje dvě pracoviště: vládní a národní CERT. Jejich úlohou je působit jako prvotní zdroj informací a pomoci pro orgány státu, organizace i občany a hrají roli i při rozvoji vzdělání o bezpečnosti na internetu. Orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti, plní povinnosti vůči vládnímu CERT týmu a orgány a osoby podle § 3 písm. a) a b) plní povinnosti zejména vůči národnímu CERT týmu.

5 Systémový přístup ke kybernetické bezpečnosti

Savage a Schneider [39] vysvětlují, že bezpečnost nelze škálovat přidáváním hardwaru nebo softwaru, ale že je to vlastnost celého systému vzešlá ze vztahů mezi jeho prvky. Tím objasňují, proč kybernetická bezpečnost potřebuje systémový přístup a na něm založenou tvorbu strategie, kterou organizace potřebují k osvojení bezpečnostních technologií a pochopení rizik.

Vzhledem k tomu, že potřeba komplexního a sofistikovaného přístupu ke kybernetické bezpečnosti je poměrně nová, zmínek o přínosech vzešlých z aplikace systémového přístupu zatím není mnoho, přestože k jeho použití kromě Savage a Schneidera nabádají i další autoři [56].

Jedna z prvních vlaštovek pochází z MIT [15], kolébky systémového přístupu, a zabývá se vyhodnocováním incidentů – oblasti, která rozhodně potřebuje rozvoj. Na MIT se zrodil bezpečnostní model STAMP (Systems-Theoretic Accident Model and Processes) založený na systémovém přístupu a určený k vyhodnocování bezpečnostních incidentů a rizik i k navrhování metodologií k jejich prevenci a metodik k jejich hodnocení.

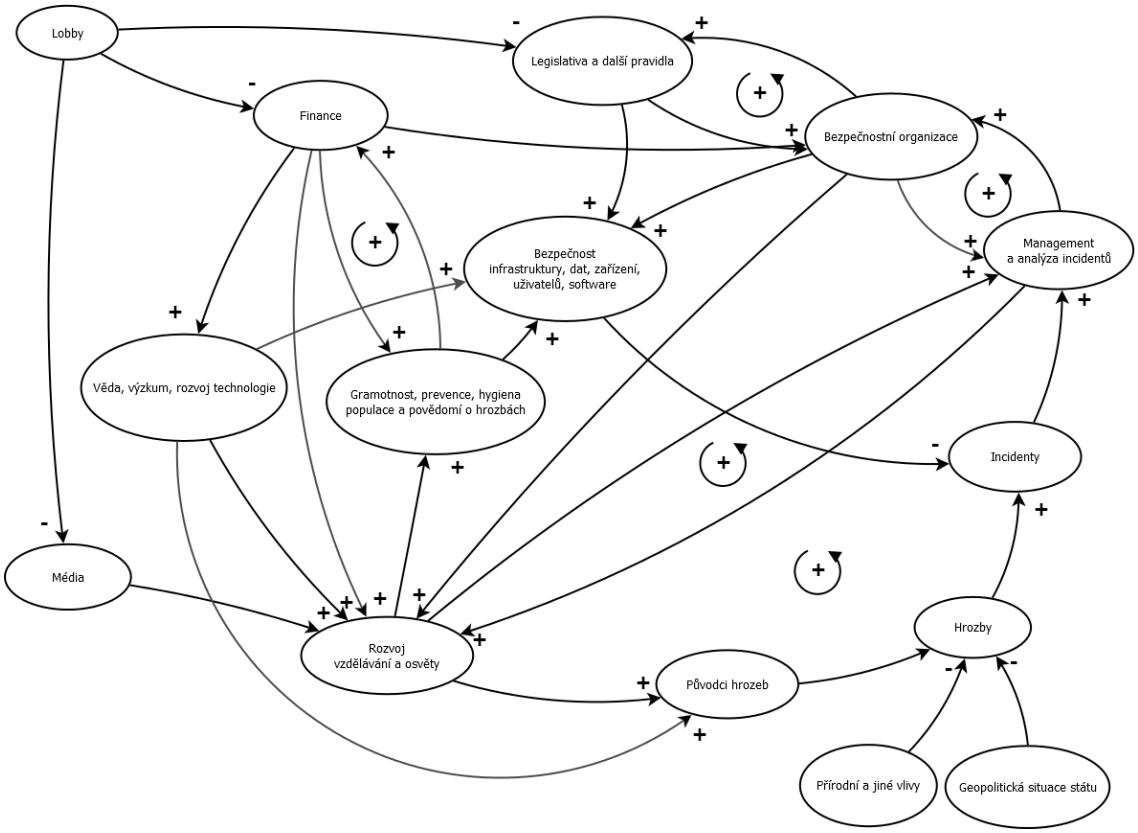
STAMP bere v úvahu omezení a hranice systému, řídící smyčky, modely procesů a úrovně řízení. Incident je považován za výsledek nedostatku omezení uvalených na návrh systému, resp. jako kulminaci komplexních procesů, a ne jednotlivých událostí. Ohled je brán i na to, že systémy jsou socio-technické, tedy že významnou roli hraje lidský faktor, který do procesu zasahuje přímo fyzicky, ale i nepřímo prostřednictvím různých pravidel a nařízení. STAMP byl aplikován na příkladech jednotlivých událostí týkajících se bezpečnosti leteckých a vojenských systémů, později byla představena možnost jeho užití v kybernetické bezpečnosti na příkladu metody CAST (Causal Analysis based on STAMP), která byla použita na analýzu incidentů a jejich příčin.

Další vlaštovkou je v roce 2015 představená metodologie CAIA (Cyber Attack Impact Assessment) k posouzení dopadů kybernetického útoku na kritickou infrastrukturu [57]. CAIA podobně jako STAMP, resp. CAST zahrnuje i lidský faktor. Metodologie porovnává chování bez incidentů a včetně incidentů, zkoumá kontrolní proměnné, pozorované proměnné a události probíhající v procesech. Nastíněny byly možnosti využití metodologie od vyhodnocování rizik až po kontrolu návrhu sítí, bylo také upozorněno možnost, že metodologii mohou zneužít i útočníci k přípravě ničivějšího útoku.

5.1 Systém kybernetické bezpečnosti ČR

Na základě analýzy z předchozí kapitoly a na základě konzultace v CSIRT.CZ (CZ.NIC) [46] byl sestaven model systému kybernetické bezpečnosti ČR. Pro reprezentaci systému byl zvolen smyčkový diagram. Znázorněny jsou pouze stěžejní prvky, smyčky a vztahy, které se povedly objasnit. Zachycení systému v celé jeho šíři a komplikovanosti je mimo rozsah této práce a bude předmětem dalšího výzkumu.

Systém interaguje s okolím, je otevřený, vyvíjí se v čase, je dynamický, lze ho rozdělit na menší měkké i tvrdé subsystémy, je tedy hierarchický. Mimo systém, ale přesto s výrazným vlivem na něj, stojí prvky: geopolitická situace státu, přírodní a jiné vlivy a lobby.



Obr. 15: Systém kybernetické bezpečnosti ČR
Zdroj: vlastní zpracování

5.1.1 Prvky systému

Vzdělávání a osvěta

Představuje veškeré vzdělávací a osvětové aktivity včetně výuky na školách. Jde tedy o souhrn školení, kurzů, cvičení a tréningů, učebních materiálů a lidských kapacit. V současnosti je většina aktivit zacílena především na správce sítí a jiné IT odborníky.

V ideálním stavu bude kvůli velké dynamice systému zapotřebí vzdělávací plány a materiály průběžně aktualizovat a zajistit kontinuální vzdělávání učitelů a školitelů. Podle agentury ENISA [21] by účinné vzdělávání o více než 50 % snížilo množství incidentů, avšak systematický přístup k osvětě a vzdělávání koncových uživatelů zatím chybí.

Gramotnost, prevence a hygiena populace

Je výsledkem vzdělávacích a osvětových aktivit. Osvícená populace (zejména její ohroženější skupiny – děti a senioři) přispívá k bezpečnosti infrastruktury, zařízení a dat.

Bezpečnost infrastruktury, zařízení, softwaru, dat, uživatelů

Tento prvek se skládá ze 2 úrovní subsystémů (nastíněných v následující kapitole 5.1.3), kde bezpečnost by měla být vlastností každého z nich.

Média

Zahrnuje tisk, rozhlas, kino, televizi, internet a další média, prostřednictvím kterých lze šířit vzdělání a osvětu. V současnosti je využíván především internet pro šíření odborných informací pro bezpečnostní specialisty, ale objevují se i dobré příklady využít televize a rádia (kapitola 4.4.2), avšak plný potenciál využití médií pro oslovení široké veřejnosti zůstává zatím nevyužit.

Incidenty

Zahrnuje veškeré bezpečnostní incidenty a trestné činy kyberkriminality.

Management incidentů

Zahrnuje sběr dat o incidentech (včetně kyberkriminality) a jejich rozbor, který v ideálním případě přináší informace i o původcích hrozeb a zahrnuje proaktivní, realtimový i reaktivní přístup, jak bylo objasněno v kapitole 4.3.2.

Věda, výzkum, rozvoj technologie

Zahrnuje aktivity na poli vědy a výzkumu. Ty přispívají k rozvoji bezpečnosti, ale také hrozeb.

Legislativa a další pravidla

Zahrnuje zákony, vyhlášky, ale také pravidla a vnitřní řády a politiku organizací (myšleno nejen bezpečnostních, tedy všech subjektů soukromých i státních, ziskových i neziskových).

V kapitole 4.5 je doložena pomoc bezpečnostních organizací s přípravou legislativy i jiných dokumentů, které dále ovlivňují činnost organizací (zatím převážně v pozitivním smyslu).

Bezpečnostní organizace

Zahrnuje organizace a jiné celky podílející se na kybernetické bezpečnosti (např. Policie ČR, NBÚ, NCKB, CSIRT/CERT týmy na úrovni státu i jednotlivých podniků nebo škol, ale také nadnárodní organizace jako ENISA či NATO). Jejich vzájemnou provázanost a spolupráci lze modelovat jako samostatný subsystém a všechny dostupné údaje nasvědčují tomu, že je na dobré úrovni.

Finance

Množství finančních prostředků nutných na zajištění fungování bezpečnostních organizací a vzdělávacích a vědeckých aktivit. Dostupnost financí může být příznivě ovlivněna povědomím populace kybernetické bezpečnosti a hrozbách.

5.1.2 Prvky mimo systém, které je potřeba brát v potaz

Hrozby

Zahrnuje všechny druhy hrozeb, jak byly popsány v kapitolách 4.1 a 4.2. Na vývoj hrozeb mají vliv jejich původci a konkrétní realizované hrozby se stávají incidenty.

Původci hrozeb

Zahrnuje původce hrozeb a dostupní informace o nich je nutné je do systému taky zahrnout, protože rozvoj technologie a vzdělávání bude mít pozitivní vliv i na jejich schopnosti a bude docházet k profesionalizaci a dělbě rolí (kapitola 4.2.1) a zřetel bude potřeba brát i na jejich vlastnosti a motivace (kapitola 4.3.2.1).

Geopolitická situace státu

Ovlivňuje druhy a možnosti hrozeb

Přírodní a jiné vlivy

Těžko ovladatelný prvek, který by ale neměl být opomenut.

Lobby

Prvek byl doplněn na základě rozhovoru v CSIRT.CZ. Uvažován je vliv na média, legislativu a finance.

5.1.3 Subsystémy z pohledu bezpečnosti

Z pohledu bezpečnosti, která je vlastností systému jako celku, je možné určit 3 subsystémy – bezpečnost musí být vlastností každého z nich. První 2 úrovně jsou na diagramu zastoupeny jedním prvkem, třetí úroveň reprezentuje diagram samotný.

Úroveň 1 (nejnižší):

Bezpečnost každého jednoho zařízení/prvku infrastruktury

Zahrnuje zabezpečení dat, SW, HW a přístupu k nim a také vzdělaného a osvíceného uživatele, který dbá na bezpečnost.

Úroveň 2 (střední):

Bezpečnost na úrovni sítě/organizace

Zahrnuje patřičně zabezpečenou podnikovou síť, proaktivní přístup vedení i zaměstnanců, kontinuální vzdělávání uživatelů, odpovídající podnikovou politiku a vnitřní pravidla, prostředky pro monitorování hrozeb a incidentů, metodiku na jejich posouzení a sdílení informací o nich s dalšími podniky a bezpečnostními organizacemi.

Úroveň 3 (nejvyšší):

Bezpečnost na úrovni státu

Zahrnuje součinnost všech soukromých i veřejných organizací na úrovni ČR i Evropy, zájem a aktivní přístup vlády a všech občanů, důraz na průběžný rozvoj vzdělávání i legislativy a dostatek financí.

5.1.4 Zhodnocení systému a systémovosti současného přístupu

Evropská unie ve zkoumaných materiálech [1] a [37] řeší kybernetickou bezpečnost komplexně, kromě konkrétních kroků např. v oblasti legislativy ale spíše rámcově. Řeší spolupráci bezpečnostních složek a organizací, průmyslu, vědecké a akademické sféry, obchodní příležitosti a zastřešení a podporu kooperaci všech složek na státní a mezistátní úrovni. Lze konstatovat, že NBÚ, resp. NCKB vidí kybernetickou bezpečnost taktéž velmi komplexně a bere v potaz dynamiku hrozeb i dalších prvků systému. I spolupráce a vazby mezi organizacemi zajišťujícími bezpečnost se ubírají dobrým směrem a postupně jsou začleňovány další organizace podílející se na vzdělávání.

Chápání dynamiky systému je vidět zejména v souvislosti s vývojem hrozeb a zaměřením na jejich analýzu (jak bylo zmíněno v kapitole 4.5.3 – správa a rozvoj laboratorního prostředí je kontinuální proces) a v souvislosti tvorbou a aktualizací významných

bezpečnostně-strategických materiálů ČR. Daleko menší důraz na dynamiku panuje v oblasti osvěty, podniknuté a do budoucna naznačené kroky v *NSKB* se zdají být spíše jednorázového charakteru a na rozvoj školství se pohlíží převážně staticky.
Je např. zmíněn záměr modernizovat stávající vzdělávací programy základních a středních škol, není ale zohledněno, že nestačí jednorázová modernizace, nýbrž že bude zapotřebí neustálý vývoj a průběžné doplňování znalostí pedagogů a školitelů. U vysokých škol je však zmíněna pouze podpora nových programů, které budou produkovat experty na kybernetickou bezpečnost. Osvěta široké veřejnosti je zmíněna jen velmi obecně. Možnostmi využití všech médií nezohledňují ani materiály EU, ani NBÚ. V důrazu na bezpečnost jako vlastnost celého systému tedy prozatím panují rezervy.
Rezervy panují také ve skloubení více vědních disciplín a prolínání s dalšími obory (prospěšnost tohoto přístupu popsána v kapitole 3.4.2). Potřebu takového přístupu obecně k ICT zmiňuje i prof. Král [26] a spěje k němu zvolna i kybernetická bezpečnost, jako příklad může posloužit výzkum původců hrozeb, popsaný v kapitole 4.3.2. Z digramu systému a popisu prvků je dobře vidět, že takový přístup by byl prospěný zejména s ohledem na zmiňovaný výzkum původců a rozvoj vzdělávání a školství, ale také na plné využití médií pro přínos k osvětě (např. i při výrobě seriálu *Nebojte se internetu*, zmíněného v kapitole 4.4.2, se ukázala potřeba odborníků rozumějících bezpečnosti, médiím a současně vzdělávání seniorů [58]).
V oblasti chápání bezpečnosti jako vlastnosti celku a důrazu na všechny prvky systému tedy prostor pro zlepšení je.

5.1.5 Porovnání se systémem veřejného zdravotnictví

V duchu poznatků Forrestera a Stermana (zmíněných v kapitole 3.3) o porozumění systémům díky přenositelnosti struktur a chování se nabízí se možnost porovnat kybernetickou bezpečnost s jinými podobnými systémy a v ideálním případě vylepšit chápání systému nebo systém samotný aplikací podobného schéma fungování.

Na kybernetickou bezpečnost je nutné pohlížet jako na evoluční systém, nikoliv účelově navržený [56],proto se nabízí srovnaní s jiným příbuzným evolučním systémem, a to s veřejným zdravotnictvím.

Jak uvádí Janečková a Hnilicová [59], veřejné zdravotnictví (též označované jako sociální lékařství nebo preventivní lékařství) tvoří komplexní systém. Oproti lékařství nezkoumá pouze zdraví konkrétního jednotlivce, ale řeší celou společnost, populační skupiny a

komunity. Je to dynamický obor, zahrnují přímo i nepřímo mnoho disciplín z oblasti medicíny, etiky, filozofie, ekonomiky a vědy o řízení, psychologie, demografie, statistiky a informatiky.

Počátky vývoje lze vysledovat až do 14. století a od rozmachu v 18. a 19. století (kdy byl v Anglii r. 1848 přijat první zdravotní zákon, tzv. Public Health Act) pokračuje vývoj systému dodnes. Během času se vyvinul systém, kde je důraz kladen na porozumění hrozbám, jejich původu a příčinám a na tom založené léčbě a preventivních opatřeních, mezi které patří i to, že základní pravidla hygieny a péče o zdraví se děti učí už od předškolního věku. Vzdělání lékařů už nezahrnuje pouze přírodovědnou orientaci, ale i témata ze společenských věd, ekonomie, informatiky, práva a dalších oborů. „*Nutností se stalo kontinuální celoživotní vzdělávání lékařů a dochází k emancipaci dalších, nelékařských zdravotnických profesí* [59]."

Dobře popsanou vlastností, která se emerguje na úrovni systému je např. skupinová imunita. Pokud v populaci převažují zdraví a proočkovaní jedinci, nemoci se hůře šíří, což poskytuje ochranu i jedincům slabším, s horším zdravotním stavem nebo neočkovaným [60].

Nutno dodat, že přestože ve zdravotnictví jsou principy principům systémového myšlení a dynamiky již uplatňovány (zpětné vazby a z nich plynoucí přímé a nepřímé příčiny; dynamika vývoje v čase), WHO [61] vidí aplikaci systémového myšlení jako jednu ze 4 revolucí, které zdravotnictví a zdravotnické systémy v brzké době změní.

Shrnuto, systém veřejného zdravotnictví klade důraz na multidisciplinaritu nezbytnou k celkovému fungování systému, na kontinuální vzdělávání, taktéž multidisciplinárně zaměřené, prevenci a hygienu. Zdraví je zde plně chápáno coby vlastnost systému jako celku (což se projevilo i tím, že některé hrozby se podařilo zcela eliminovat a jiné značně potlačit či poměrně účinně se s nimi vypořádat).

Oblast kybernetické bezpečnosti se tedy v mnohém může od veřejného zdravotnictví učit. Uvědomění si podobností příslušnými organizacemi a vládami států by mohlo celý vývoj posunout dobrým směrem.

5.2 Dynamický model

5.2.1 Dostupná data

Na detailní kvantitativní popis kybernetických hrozeb a bezpečnosti v současné době není dostatek kvalitních dat. Dostupná data buď nemají vypovídající hodnotu, nebo jsou neúplná, nebo jde o odhady. V blízké budoucnosti lze předpokládat výrazné zlepšení. U analýzy incidentů hrají roli zatím neustálené metodiky jejich hodnocení (které jsou, jak již bylo několikrát zmíněno, stále ve vývinu a blízké budoucnosti lze čekat jejich ustálení), finanční a jiné dopady incidentů jsou tak zatím pouhé odhady.

Statistiky jednotlivých hrozeb většinou zveřejňují společnosti působící na poli počítačové bezpečnosti, ale často se týkají jen sítí, které spravují nebo hrozeb, které jejich antivirový software odhalil. Společnosti mají tendence navazovat partnerství a spolupracovat (zmíněno v kapitole 4.3.1) a do příštích let metodiky měření a statistiky sjednocovat.
Podle údajů společnosti McAfee [38] v letech 2014 a 15 rostl počítačový i mobilní malware, výrazně rostl malware na Mac OS a také ransomware, u kterého se předpokládá další růst i do budoucna. Množství ransomware v roce 2015 podle údajů společnosti Symantec [62] stouplo o 35 % a nově se objevil i na mobilech. Současně v mobilní sféře přibylo 214 % nových zranitelností. Časté byly úniky osobních údajů ve zdravotnictví a dalších oborech, celkově bylo v roce 2015 přes půl miliardy osobních záznamů ukradeno nebo ztraceno, Symantec ale podotýká, že se patrně jedná jen o pomyslnou špičku ledovce.

Eurostat i ČSÚ poskytují k tématu ICT široké spektrum velice základních statistik o připojení k internetu jednotlivců a domácností, typu připojených zařízení, využití eGovernmentu, elektronického obchodování, podílu zaměstnanců v IT službách na celkové zaměstnanosti atd. Bohužel komplexnější statistiky týkající se kybernetických hrozeb chybí, nebo jsou velmi obecné [63] a často obsahují jen data za roky 2010 a 2015. ČSÚ zkoumal hrozby a bezpečnost pouze ve zmíněných letech na základě iniciativy Eurostatu (a naneštěstí místo detailnějších a použitelnějších údajů o hrozbách, bezpečnosti ohrožených skupin a vývoji digitální gramotnosti v rámci populace ČSÚ zkoumal např. velikost obce, ze které respondenti pocházeli). Teprve v roce 2016 nastal drobný posun, když ČSÚ v reakci na současné trendy aktualizoval a rozšířil typy zkoumaných veličin a indikátorů mj. např. o to, kdo v podnicích řeší bezpečnost dat [30]. Ke zlepšení tedy postupně dochází a lze doufat, že tomu tak bude i v budoucnu.

Bezpečnostní týmy GOVCERT.cz a CSIRT.CZ zveřejňují statistiky zjištěných incidentů. Statistiky celkového počtu incidentů sice určitou vypovídající hodnotu mají, jak ale vyplynulo z rozhovoru v CZ.NIC [46], jsou zatížené zkreslením, protože jedno hlášení může zahrnovat od jedné do tisíců IP adres a je klasifikováno jako 1 incident. Správnější by bylo klasifikovat incidenty podle IP adres, což CSIRT.CZ plánuje do budoucna.
Policie zveřejňuje statistiku zjištěných činů kyberkriminality od roku 2011(Graf v kapitole 4.2.1), včetně rozdělení do nejpočetnějších skupin trestných činů. Všechny zjištěné hodnoty jsou zatíženy vysokou mírou latence (zmíněno v téže kapitole).

5.2.2 Modelování kyberkriminality

Pro předvedení možnosti dynamické simulace byl zvolen vývoj počtu trestných činů kyberkriminality. Celkový počet incidentů závisí na více veličinách, z nichž ty hlavní lze vyčíslit již poměrně přesně, jiné v současnosti zatím vyčíslit nelze. Přestože analýza hrozeb ukázala, že mnoho druhů hrozeb je na internetu nezávislých, mnohem více jich je s internetem spojeno a s jeho rostoucím využitím poroste i nebezpečí. Z jednotlivců i podniků používajících internet jsou nejrizikovější ty nezabezpečené. Proto byl do modelu zahrnut vývoj počtu připojených podniků a jednotlivců včetně jejich zabezpečení. Vývoj počtu incidentů závisí také na počtu připojených zařízení, které hlavně v rámci IoT mají chabé zabezpečení. Po vynásobení podílem nezabezpečených uživatelů, resp. podniků dostáváme počet nejzranitelnějších zařízení, vhodných k útoku, jejich celkové počty lze vyjádřit vztahy:

$$P_j = (Míra\ ohrožených\ uživatelů\ \cdot Podíl\ připojených\ uživatelů\ ) \cdot Zařízení\ uživatelů$$
$$P_p = (Míra\ ohrožených\ podniků\ \cdot Podíl\ připojených\ podniků\ ) \cdot Zařízení\ podniků$$

Roční přírůstek trestných činů lze popsat rovnicí:

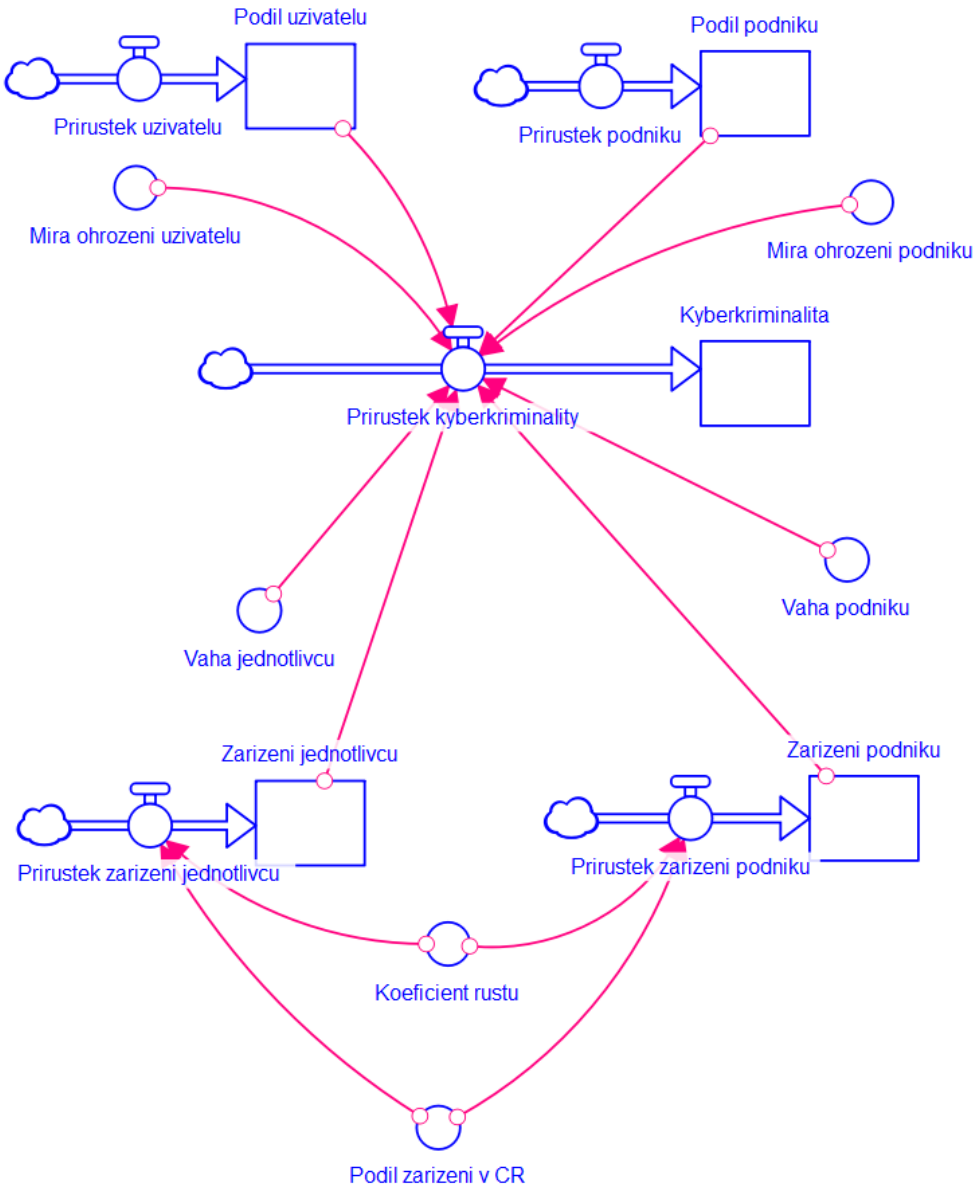
$$y = (a \cdot P_j) + (b \cdot P_p) + (c \cdot P_x)$$

kde na základě regrese byly určeny členy k a q, reprezentující váhy jednotlivých veličin a člen $(c \cdot P_x)$, který je možné interpretovat jako další příčiny kyberkriminality, v současnosti matematicky nepopsatelné.

Statistiky kybernetické kriminality Policie ČR zveřejnuje od roku 2011, tento rok byl proto zvolen jako počátek simulace. Simulace je provedena od roku 2017 na dalších 5 let, vzhledem rychlému vývoji ICT nelze provádět dlouhodobější předpovědi.

5.2.3 Prvky modelu:

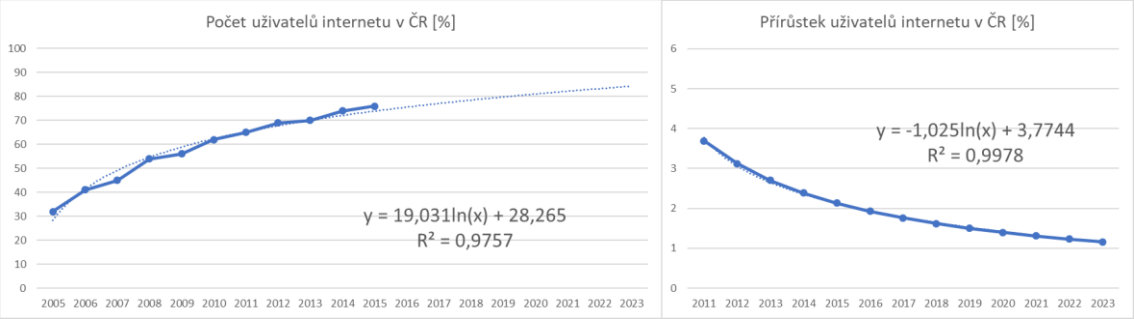
Model popisuje vývoj sledovaných veličin pomocí ročních přírůstků celkového počtu. Přestože u každé veličiny dochází i k úbytku (jak ostatně dokládá i vývoj podniků), všechny dostupné zdroje se zabývají pouze celkovým počtem v daném období a proto i odvozený výpočet přírůstků z něj musel vycházet.



Obr. 16: Dynamický model kyberkriminality
Zdroj: vlastní zpracování

Podíl uživatelů

Vyjadřuje vývoj počtu jednotlivců používajících internet, vychází z údajů ČSÚ [64], který do podílu zahrnuje všechny obyvatele ve věku od 16 let. Z údajů Eurostatu [65] o vyspělejších státech vyplývá, že růst se směrem k hranici 100 % zvolní a ustálí (v Lucembursku, Nizozemí a Norsku se ustálil na hodnotách okolo 96 nebo 97 %).

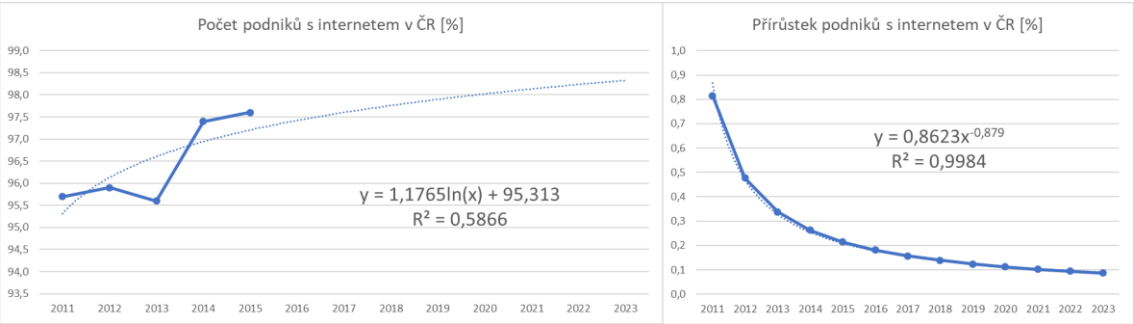


Obr. 17: Vývoj počtu uživatelů internetu v ČR
Zdroj: vlastní zpracování

Podíl podniků

Vyjadřuje podíl podniků připojených k internetu. Přestože míra připojení velkých podniků se blíží 100 %, malé podniky zaostávají a právě nově připojené a nezabezpečené (resp. jejich zařízení) se mohou stát terčem útoku.

Průměrný podíl všech podniků byl stanoven na základě dat ČSÚ [30] jako vážený průměr jednotlivých podniků podle jejich velkosti, kde vahami jsou četnosti podniků v dané skupině.



Obr. 18: Vývoj počtu podniků s internetem v ČR
Zdroj: vlastní zpracování

Míra ohrožení podniků

Koeficient vychází z jediného dostupného údaje, z průzkumu ČSÚ z roku 2016 [29], podle kterého 20,5 % podniků neřeší zabezpečení dat a patří tedy mezi nevíce ohrožené.

Míra ohrožení jednotlivců

Koeficient je stanoven podle jediného dostupného údaje ČSÚ z roku 2010 [64], kdy bylo zjištěno že 23 % uživatelů neví, jak mají zabezpečen počítač, což lze interpretovat tak, že postrádají přehled o kybernetických hrozbách i základní míru digitální gramotnosti a právě oni, resp. jejich zařízení jsou nejvíce ohrožena.

Kyberkriminalita

Představuje celkový počet trestných činů kybernetické kriminality od počátku simulace.

Přírůstek kyberkriminality

Přestavuje roční počet trestných činů kybernetické kriminality.

Zařízení jednotlivců a zařízení podniků

Představuje počet zařízení připojených k internetu používaných jednotlivci/podniky v milionech kusů. Použité funkce popisují počet pro celý svět násobený podílem zařízení v ČR, přičemž poměr zařízení podniků a jednotlivců zůstává stejný.

Vývoj veličiny je založený na údajích společností Gartner [66], která předpokládá exponenciální růst celkového počtu zařízení z 3,9 miliard v roce 2014 přes 6,4 miliard v roce 2016 až na 20,8 miliard v roce 2020.

Podíl počtu zařízení v ČR

Koeficient vyjadřující část celkového počtu zařízení ve světě, která připadají na ČR. Vychází z počtu zařízení na 1 obyvatele ČR. Společnost Symantec s využitím zmíněné předpovědi Gartneru uvedla, že v USA připadalo v roce 2016 na 1 obyvatele 0,25 zařízení, podle údajů ze statista.com [67] to bylo 2,9 zařízení na osobu už v roce 2014. Stejný zdroj uvádí pro Německo hodnotu 2,4. Ve výchozím nastavení simulace byl počet zařízení na 1 obyvatele ČR (s větším důrazem na hodnoty Symantecu kvůli jejich kompatibilitě s údaji Gartneru) aproximován na 0,5 na osobu v roce 2011, podle populačních dat ČSÚ [68].

Koeficient růstu

Umožňuje při simulaci regulovat přírůstek počtu zařízení. Při výchozí hodnotě 1 nemá žádný vliv.

5.2.4 Výsledky simulace

Výsledky simulace při výchozím nastavení řádově korespondují se statistikami Policie ČR a pro uplynulé roky. Kvůli zmiňované latenci, pro jejíž namodelování v současnosti nejsou žádné údaje, a kvůli prozatímní nevyčíslitelnosti dalších dílčích příčin kyberkriminality není bližší shoda údajů možná. Model je připraven na budoucí upřesnění některých prvků podle nově dostupných nebo zjištěných skutečností.

První simulace předpokládá všechny prvky v základním nastavení, tedy od roku 2016 prudký růst počtu zařízení v souladu s předpovědí Gartneru. Druhá simulace znázorňuje pomalejší vývoj zařízení v budoucích letech a také bere v úvahu vývoj míry ohrožení jedinců a podniků v čase, s přihlédnutím k postupnému rozvoji vzdělávacích aktivit a vývoji populace bylo modelováno celkové zlepšení o 10 % v koncovém roce simulace.

Table 1 (Zakladni nastaveni)

Years	Prirustek zari	Zarizeni podn	Prirustek zari	Zarizeni jedno	Prirustek kyb
1	0,28	0,94	0,45	1,31	2†009,49
2	0,37	1,22	0,61	1,76	2†390,19
3	0,48	1,59	0,82	2,37	2†893,48
4	0,63	2,08	1,11	3,19	3†560,76
5	0,82	2,71	1,49	4,30	4†446,44
6	1,07	3,52	2,01	5,79	5†622,61
7	1,39	4,59	2,71	7,80	7†185,07
8	1,81	5,98	3,64	10,51	9†261,16
9	2,36	7,79	4,91	14,15	12†020,20
10	3,07	10,15	6,61	19,06	15†687,40
11	4,00	13,22	8,90	25,67	20†562,30
12	5,21	17,22	11,99	34,57	27†043,42

Obr. 19: Výsledky simulace v základním nastavení
Zdroj: vlastní zpracování

Table 2 (Pomalejsi vyvoj)

Years	Prirustek zari	Zarizeni podn	Prirustek zari	Zarizeni jedno	Prirustek kyb
1	0,28	0,94	0,45	1,31	2†010,07
2	0,37	1,22	0,61	1,76	2†391,01
3	0,48	1,59	0,82	2,37	2†906,16
4	0,63	2,08	1,11	3,19	3†578,51
5	0,82	2,71	1,49	4,30	4†471,13
6	1,03	3,52	1,94	5,79	5†563,52
7	0,80	4,55	1,55	7,73	6†361,95
8	0,86	5,35	1,73	9,28	6†920,59
9	0,94	6,21	1,96	11,01	7†171,21
10	1,08	7,15	2,33	12,97	7†618,57
11	1,25	8,23	2,79	15,30	7†944,68
12	1,52	9,49	3,49	18,09	8†301,70

Obr. 20: Výsledky simulace s pomalejším vývojem zařízení a klesající mírou ohrožení
Zdroj: vlastní zpracování

Pro současný model je limitující zejména krátké období, ze kterého pocházejí vstupní data. Nejen delší časové období sběru dat by pomohlo ke zlepšení. Model by byl podstatně přínosnější, pokud by byl dostatek dat ke zkoumání jednotlivých skupin podniků podle velikosti, protože nejvíce ohrožené jsou malé a střední podniky (doloženo v kapitole 4.2) a pokud by mohl být zkoumán vývoj povědomí a gramotnosti v oblasti počítačové bezpečnosti v rámci populace ČR rozdělené podle věkových skupin, se zaměřením na ty nejzranitelnější – děti a seniory. Bohužel, přístup dětí k ICT a internetu zkoumal ČSÚ pouze v roce 2010 [64] a dál mu nevěnuje pozornost.

6 Shrnutí výsledků, závěry a doporučení

Z analýzy vyplynulo, že současný přístup dobře využívá příkladné spolupráce všech zainteresovaných organizací na úrovni ČR i EU. Naopak rezervy současného přístupu jsou jednak v nedostatečném důrazu na přínosy vzdělání a osvěty a na multidisciplinární přístup, který chybí oboru ICT obecně, a na možnosti inspirace v jiných systémech.
Dynamická simulace modelu kyberkriminality pomohla nastínit budoucí vývoj a ukázala, že pokud se naplní uvažované předpovědi růstu počtu zařízení, dojde k velkému růstu počtu trestných činů. Naopak při předpokladu rozvoje osvěty a mírnějšího růstu simulace ukázala, že vývoj počtu trestných činů bude mírnější a zvladatelnější.

Oblast ICT přináší každý rok mnoho změn, proto bude nezbytné modely v budoucnu dále doplňovat o nové prvky a zpřesňovat podle aktuální situace. Lze očekávat, že v dohledné době dojde k ustálení metod vyhodnocování incidentů a že díky užší spolupráci všech subjektů vzniknou souhrnnější, ucelenější a podrobnější statistiky na státní nebo evropské úrovni. Bude tedy možné identifikovat další vztahy, matematicky je popsat, zahrnout do dynamického modelu a dostat se k přesnějším výsledkům, které umožní prakticky zkoumat mnoho aspektů kybernetické bezpečnosti, například dopad incidentů na lokální i státní úrovni, rozvoj vzdělávání a finanční nebo personální náročnost.
Bylo by také vhodné analyzovat vývoj systémů nejen kybernetické bezpečnosti ve vyspělejších státech a prozkoumat možnosti adaptace vybraných prvků do českého prostředí.
V dalším studiu považuje autor za důležité shromážděné informace dál šířit, např. prostřednictvím webu, a přispět k tolik potřebné osvětě. Dále prozkoumat možnosti rozšíření sledovaných statistických ukazatelů a díky zpřesnění modelů určovat např. finanční náročnost boje s kyberkriminalitou, nebo pomocí modelování rozvoje míry vzdělanosti, osvěty a dalších preventivních opatření v rámci věkových skupin populace zkoumat možnosti redukce hrozeb.

7 Seznam použitých zdrojů

[1] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [online]. 2013 [cit. 2017-02-28]. Dostupné z: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[2] PETERS, David. The application of systems thinking in health: why use systems thinking?. *Health Research Policy and Systems*. 2014, **12**(1), -. DOI: 10.1186/1478-4505-12-51. ISSN 1478-4505. Dostupné také z: http://health-policy-systems.biomedcentral.com/articles/10.1186/1478-4505-12-51

[3] STRIJBOS, S. a Andrew BASDEN. *In search of an integrative vision for technology: interdisciplinary studies in information systems*. 1st ed. New York: Springer, 2006. ISBN 03-873-2162-4.

[4] Internetová jazyková příručka – systém. *Internetová jazyková příručka* [online]. b.r. [cit. 2016-11-04]. Dostupné z: http://prirucka.ujc.cas.cz/?slovo=systém

[5] BUREŠ, Vladimír. *Systémové myšlení pro manažery*. Vyd. 1. Praha: Professional Publishing, 2011. ISBN 978-80-7431-037-9.

[6] CAPRA, Fritjof. *Tkáň života: Nová syntéza mysli a hmoty*. Vyd. 1. Praha: Academia, 2004. ISBN 80-200-1169-2.

[7] *Modeling and Simulation in the Systems Engineering Life Cycle*. Springer-Verlag New York Inc, 2015. ISBN 978-144-7156-338.

[8] ŠTĚCHA, Jan a Vladimír HAVLENA. *Teorie dynamických systémů* [online]. 2005 [cit. 2016-25-011]. Dostupné z: https://moodle.dce.fel.cvut.cz/mod/resource/view.php?id=486

[9] MILDEOVÁ, Stanislava. *Systémová dynamika: tvorba modelu*. Vyd. 1. Praha: Oeconomica, 2011. ISBN 978-80-245-1842-8.

[10] FORRESTER, Jay. *Some Basic Concepts in System Dynamics* [online]. 2009 [cit. 2016-12-07]. Dostupné z: http://static.clexchange.org/ftp/documents/system-dynamics/SD2009-02SomeBasicConcepts.pdf

[11] STERMAN, John. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. [Nachdr.]. Boston: Irwin/McGraw-Hill, 2000. ISBN 00-723-8915-X.

[12] CHEN, Huey. Interfacing theories of program with theories of evaluation for advancing evaluation practice: Reductionism, systems thinking, and pragmatic synthesis. *Evaluation and Program Planning*. 2016, **59**, 109-118. DOI: 10.1016/j.evalprogplan.2016.05.012. ISSN 01497189. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/S0149718916301008

[13] RICHMOND, Barry. *System Dynamics/Systems Thinking: Let's Just Get On With It* [online]. In: . 1994 [cit. 2017-02-04]. Dostupné z: https://www.iseesystems.com/resources/articles/download/lets-just-get-on-with-it.pdf

[14] PROROK, Vladimír. *Tvorba rozhodování a analýza v politice*. Vyd. 1. Praha: Grada, 2012. ISBN 978-80-247-4179-6.

[15] SALIM, Hamid M. *Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks* [online]. Massachusetts Institute of Technology, 2014 [cit. 2017-05-02]. Dostupné z: http://ic3.mit.edu/ResearchSamples/2014-07.pdf.

[16] FORRESTER, Jay. *System Dynamics - the Next Fifty Years* [online]. 2007 [cit. 2016-12-08]. Dostupné z: http://static.clexchange.org/ftp/documents/system-dynamics/SD2007-08SDTheNext50Years.pdf

[17] FORRESTER, Jay. *System Dynamics: the Foundation Under Systems Thinking* [online]. 2010 [cit. 2016-12-07]. Dostupné z: http://static.clexchange.org/ftp/documents/system-dynamics/SD2011-01SDFoundationunderST.pdf

[18] FORRESTER, Jay Wright. *The Beginning of System Dynamics* [online]. In: . 1989 [cit. 2016-11]. Dostupné z: http://web.mit.edu/sysdyn/sd-intro/D-4165-1.pdf

[19] About Us. *Isee systems* [online]. b.r. [cit. 2017-01-25]. Dostupné z: http://www.iseesystems.com/about.aspx

[20] *ENISA Threat Landscape 2015* [online]. 2016 [cit. 2017-02-18]. Dostupné z: https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport

[21] *ENISA Threat Landscape Report 2016* [online]. 2017 [cit. 2017-02-20]. DOI: 10.2824/92184. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport

[22] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. In: . [cit. 2017-02-02]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[23] *Bezpečnostní strategie České republiky* [online]. In: . 2015 [cit. 2017-02-04]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[24] *Bílá kniha o obraně* [online]. In: . 2011 [cit. 2017-02-04]. Dostupné z: http://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/bila-kniha-o-obrane-190511_1.pdf

[25] BALABÁN, Miloš a Bohuslav PERNICA. *Bezpečnostní systém ČR: problémy a výzvy*. Vydání první. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. ISBN 978-80-246-3150-9.

[26] KRÁL, Jaroslav. *Výzvy, hrozby a úzká místa informatiky* [online]. MFF UK Praha, b.r. [cit. 2017-03-28]. Dostupné z: http://www.cs.cas.cz/hsi1/clanky/kral.pdf

[27] *Situační zpráva o vybraných oblastech bezpečnosti za období 1. července do 31. prosince 2014: energetická bezpečnost, bezpečnost finančních institucí, informační technologie a kybernetická bezpečnost, krizové řízení* [online]. Odbor bezpečnostní politiky Ministerstva vnitra, 2015 [cit. 2017-03-16]. Dostupné z: http://www.mvcr.cz/soubor/situacni-zprava-o-vybranych-oblastech-bezpecnosti-2014-ii.aspx

[28] Informační technologie v podnikatelském sektoru. *Český statistický úřad* [online]. b.r. [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/documents/10180/23170386/1_it_podniky_cz_2016_fin.xlsx/84c03389-c8bf-410d-95c9-dc2ca3d04c70?version=1.1

[29] Informační společnost v číslech - 2016. *Český statistický úřad* [online]. b.r. [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/documents/10180/43344124/061004-16_D.xlsx/4cbc12c2-fb7e-45d9-81da-1a70d07a3af8?version=1.1

[30] Informační technologie v podnikatelském sektoru. *Český statistický úřad* [online]. b.r. [cit. 2017-03-29]. Dostupné z: https://www.czso.cz/csu/czso/podnikatelsky_sektor

[31] Kyberkriminalita. *Policie ČR* [online]. b.r. [cit. 2017-04-01]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx

[32] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.

[33] Kriminalita – trestné činy. *Český statistický úřad* [online]. b.r. [cit. 2017-04-01]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/index.jsf?page=vystup-objekt&z=T&f=TABULKA&katalog=31008&pvo=KRI05&str=v32&s=v40__FST_FUNKCE__7503__90v40__PST_POJEM__7648__2v40__KMJ_KATEG__7501__1103

[34] European Cybercrime Centre - EC3. *Europol* [online]. b.r. [cit. 2017-03-15]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[35] *NATO - Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers, 14-Jun.-2016* [online]. b.r. [cit. 2017-01-25]. Dostupné z: http://www.nato.int/cps/en/natohq/opinions_132349.htm

[36] *Fact Sheet - NATO Cyber Defence (December 2016)* [online]. b.r. [cit. 2017-01-25]. Dostupné z: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_12/20161201_1612-factsheet-cyber-defense-en.pdf

[37] *Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign And Security Policy* [online]. 2016 [cit. 2017-02-28]. Dostupné z: https://europa.eu/globalstrategy/en/file/441/download?token=KVSh5tDI

[38] *McAfee Labs Threats Report: March 2016* [online]. Intel Security, 2016 [cit. 2017-03-15]. Dostupné z: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

[39] SAVAGE, Stefan a Fred SCHNEIDER. *Security is Not a Commodity: The Road Forward for Cybersecurity Research* [online]. 2009 [cit. 2017-02-28]. Dostupné z: http://cra.org/ccc/wp-content/uploads/sites/2/2015/05/Cybersecurity.pdf

[40] *Understanding Cyberthreat Motivations to Improve Defense* [online]. Intel Security and Privacy Office, 2015 [cit. 2017-03-24]. Dostupné z: http://simplecore.intel.com/itpeernetwork/wp-

content/uploads/sites/38/2016/10/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf

[41] Zákon o kybernetické bezpečnosti. *CSIRT.CZ* [online]. b.r. [cit. 2017-03-28]. Dostupné z: https://www.csirt.cz/page/3397/zakon-o-kyberneticke-bezpecnosti/

[42] Vyhláška o kybernetické bezpečnosti. *Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2017-03-27]. Dostupné z: https://www.govcert.cz/cs/faq/vyhlaska-o-kyberneticke-bezpecnosti/

[43] *Zpráva o stavu kybernetické bezpečnosti České republiky 2016* [online]. 2017 [cit. 2017-04-21]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/publikace/2521-zprava-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2016

[44] Jak na Internet. *Jak na Internet* [online]. b.r. [cit. 2017-04-01]. Dostupné z: https://www.jaknainternet.cz/

[45] *Zpráva o stavu kybernetické bezpečnosti České republiky 2015* [online]. b.r. [cit. 2017-03-14]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/publikace/2497-zprava-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2015

[46] DURAČINSKÁ, Zuzana. *Osobní rozhovor s bezpečnostní expertkou CSIRT.CZ*. Praha, sídlo CZ.NIC 23.3.2017.

[47] VŠ obory v oblasti kyber bezpečnosti. *Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2017-03-14]. Dostupné z: https://www.govcert.cz/cs/vzdelavani/vs-obory-v-oblasti-kyber-bezpecnosti/

[48] Cyber/ICT Security. *OSCE* [online]. b.r. [cit. 2017-03-17]. Dostupné z: http://www.osce.org/secretariat/cyber-ict-security

[49] Agentura Evropské unie pro bezpečnost sítí a informací (ENISA). *European Union website, the official EU website - European Commission* [online]. b.r. [cit. 2017-03-15]. Dostupné z: https://europa.eu/european-union/about-eu/agencies/enisa_cs

[50] Meeting of Central European Cyber Security Platform 2014. *European Union Agency for Network and Information Security* [online]. b.r. [cit. 2017-03-15]. Dostupné z: https://www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014

[51] Central European Cyber Security Platform 2014. *Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2017-03-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2140-central-european-cyber-security-platform-2014/

[52] Úvod. *Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2017-03-14]. Dostupné z: https://www.govcert.cz/

[53] CZ.NIC ohlídá kybernetickou bezpečnost České republiky. *CZ.NIC* [online]. b.r. [cit. 2017-02-26]. Dostupné z: https://www.nic.cz/page/830/cz.nic-ohlida-kybernetickou-bezpecnost-ceske-republiky/

[54] DURAČINSKÁ, Zuzana. Bezpečnostní týmy v Evropě i ve světě. *Security World* [online]. IDG Czech Republic, a. s., 2017, (12017), 40–41 [cit. 2017-03-28]. Dostupné z: https://www.nic.cz/files/nic/doc/SW_CSIRT_032017.pdf

[55] Trusted Introducer : Directory : Team Database. *Trusted Introducer* [online]. b.r. [cit. 2017-03-28]. Dostupné z: https://www.trusted-introducer.org/directory/country_LICSA.html

[56] MILLER, William. Systems Thinking for a Secure Digital World. *CrossTalk*. 2012, **25**(5), 11–14. ISSN 2160-1593.

[57] *A System Dynamics Approach for Assessing the Impact of Cyber Attacks on Critical Infrastructures* [online]. 2015 [cit. 2017-02-28]. DOI: http://dx.doi.org/10.1016/j.ijcip.2015.04.001. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1874548215000244

[58] PÍSEK, Ondřej. Internet pro dříve narozené. *Blog zaměstnanců CZ.NIC* [online]. 2016 [cit. 2017-03-01]. ISSN 2533-4727. Dostupné z: http://blog.nic.cz/2016/10/17/internet-pro-drive-narozene/

[59] JANEČKOVÁ, Hana a Helena HNILICOVÁ. *Úvod do veřejného zdravotnictví*. Vyd. 1. Praha: Portál, 2009. ISBN 978-80-7367-592-9.

[60] METCALF, C.J.E., M. FERRARI, A.L. GRAHAM a B.T. GRENFELL. Understanding Herd Immunity. *Trends in Immunology* [online]. 2015, **36**(12), 753–755 [cit. 2017-05-01]. Dostupné z: https://doi.org/10.1016/j.it.2015.10.004

[61] *Systems Thinking for Health Systems Strengthening* [online]. World Health Organization, 2009 [cit. 2017-03-28]. Dostupné z: http://www.who.int/iris/bitstream/10665/44204/http://apps.who.int//iris/bitstream/10665/44204/1/9789241563895_eng.pdf

[62] *Internet Security Threat Report* [online]. Symantec Corporation, 2016 [cit. 2017-02-26]. Dostupné z: https://www.symantec.com/security-center/threat-report

[63] Security related problems experienced through using the internet for private purposes. *Eurostat* [online]. b.r. [cit. 2017-02-29]. Dostupné z: http://ec.europa.eu/eurostat/web/products-datasets/-/isoc_cisci_pb

[64] Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2010. *Český statistický úřad* [online]. b.r. [cit. 2017-03-28]. Dostupné z: https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-domacnostech-a-mezi-jednotlivci-2010-84lk2q0621

[65] Level of internet access. *Eurostat* [online]. b.r. [cit. 2017-03-01]. Dostupné z: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00134&plugin=1

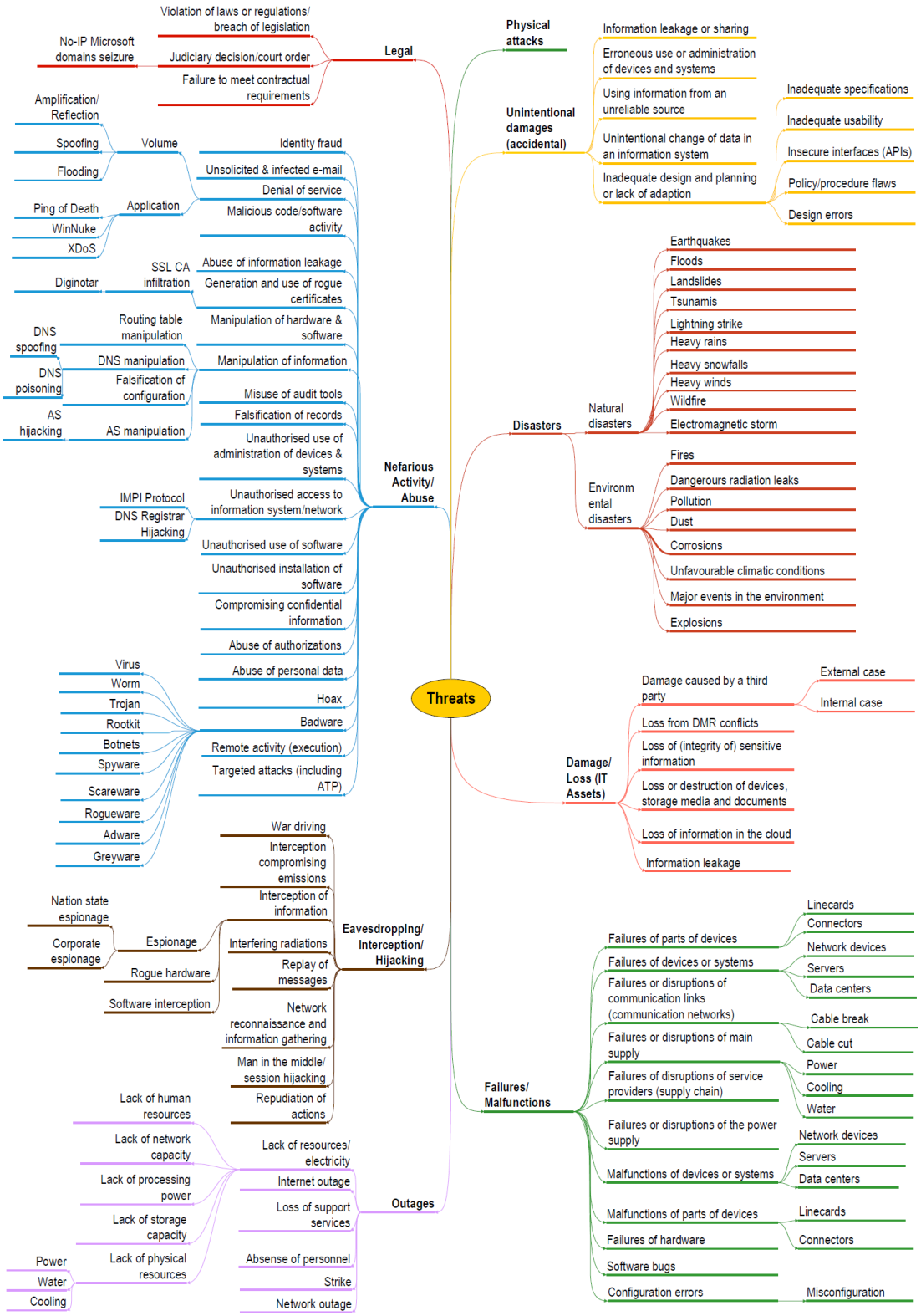
[66] Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016. *Gartner* [online]. 2015 [cit. 2017-03-28]. Dostupné z: http://www.gartner.com/newsroom/id/3165317

[67] Number of Connected Devices per Person in Selected Countries in 2014. *Statista.com* [online]. b.r. [cit. 2017-04-10]. Dostupné z: https://www.statista.com/statistics/333861/connected-devices-per-person-in-selected-countries/

[68] Věkové složení obyvatelstva - 2011. *Český statistický úřad* [online]. b.r. [cit. 2017-04-10]. Dostupné z: https://www.czso.cz/documents/10180/20555889/400312007.xls/39d43a82-0b1c-43db-bfac-37a72ef14b8b?version=1.0

8 Přílohy

1) Taxonomie kybernetických hrozeb podle agentury ENISA. Převzato z [20].



2) Taxonomie původců hrozeb podle společnosti Intel. Převzato z [40].

MOTIVATIONS OF THE REFERENCE LIBRARY OF THREAT AGENTS[4]

REFERENCE AGENT LABEL	DEFINING MOTIVATION	CO-MOTIVATION	SUBORDINATE MOTIVATION(S)	BINDING MOTIVATION	PERSONAL MOTIVATION
Civil Activist	• Ideology		• Organizational Gain	• Ideology	• Ideology
Radical Activist	• Ideology		• Dominance • Organizational Gain	• Ideology	• Ideology
Anarchist	• Ideology	• Unpredictable		• Ideology	• Ideology
Competitor	• Organizational Gain			• Organizational Gain	• Personal Financial Gain
Corrupt Government Official	• Personal Financial Gain				• Personal Financial Gain
Cybervandal	• Dominance		• Personal Satisfaction	• Dominance	• Dominance
Data Miner	• Organizational Gain			• Organizational Gain	• Personal Financial Gain
Disgruntled Employee	• Disgruntlement	• Personal Satisfaction	• Dominance • Ideology • Personal Financial Gain		• Disgruntlement
Government Cyberwarrior	• Dominance			• Dominance	• Ideology • Personal Financial Gain • Personal Satisfaction
Government Spy	• Ideology			• Ideology	• Ideology • Personal Financial Gain • Personal Satisfaction
Internal Spy	• Personal Financial Gain	• Ideology		• Personal Financial Gain	• Coercion • Ideology • Personal Financial Gain
Irrational Individual	• Unpredictable				
Legal Adversary	• Dominance			• Dominance	• Personal Financial Gain • Notoriety
Mobster	• Organizational Gain	• Dominance		• Organizational Gain	• Personal Financial Gain • Coercion
Sensationalist	• Notoriety			• Notoriety	
Terrorist	• Ideology	• Disgruntlement	• Dominance • Organizational Gain	• Ideology	• Ideology
Thief	• Personal Financial Gain			• Personal Financial Gain	• Personal Financial Gain • Personal Satisfaction
Vendor	• Organizational Gain			• Organizational Gain	• Personal Financial Gain

3) Šetření Eurostatu: Security related problems experienced through using the internet for private purposes [63]

	Podíl osob, které v posledním roce použily internet a chytily virus nebo jinou počítačovou infekci vedoucí ke ztrátě dat nebo času		Podíl osob, které v posledním roce použily internet a u kterých došlo ke zneužití osobních informací	
	2010	**2015**	**2010**	**2015**
European Union (28 countries)	31	21	4	3
European Union (27 countries)	31	21	4	3
European Union (25 countries)	31	:	4	:
European Union (15 countries)	30	20	4	4
Euro area (EA11-2000, EA12-2006, EA13-2007, EA15-2008, EA16-2010, EA17-2013, EA18-2014, EA19)	30	21	4	4
Belgium	32	20	3	3
Bulgaria	58	28	7	4
Czech Republic	26	8	1	1
Denmark	29	23	4	3
Germany (until 1990 former territory of the FRG)	22	14	2	3
Estonia	42	26	4	3
Ireland	15	11	2	1
Greece	34	25	3	2
Spain	33	25	7	5
France	34	29	5	3
Croatia	33	41	2	3
Italy	45	24	6	6
Cyprus	34	14	1	1
Latvia	41	17	5	1
Lithuania	34	19	2	1
Luxembourg	28	23	5	4
Hungary	46	36	4	3
Malta	50	28	4	8
Netherlands	23	6	6	3
Austria	14	14	3	3
Poland	30	25	3	3
Portugal	37	33	4	4
Romania	:	:	5	5
Slovenia	37	16	1	1
Slovakia	47	9	3	3
Finland	20	14	1	2
Sweden	31	19	1	3
United Kingdom	31	17	4	3
Iceland	17	:	2	:
Norway	28	13	3	3
Former Yugoslav Republic of Macedonia, the	68	71	7	5
Serbia	:	34	:	6
Turkey	36	27	4	5

4) Šetření ČSÚ: Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci – 2010 [64]

Problémy spojené s užíváním internetu, 2. čtvrtletí 2010

	Problémy, se kterými se uživatelé internetu setkali v uplynulém roce									
	infikování počítače virem nebo jiným škodlivým softwarem		nevyžádaná elektronická pošta (spam)		zneužití osobních údajů		finanční ztráty v důsledku odpovědi na podvodné zprávy (phishing) či přesměrování na podvodné stránky (pharming)		finanční ztráty v důsledku zneužití platební karty	
	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]
Celkem 16+	1 462,5	26,8	2 640,6	48,4	56,3	1,0	14,3	0,3	18,8	0,3
Celkem 16–74 let	1 453,8	26,8	2 622,5	48,3	56,3	1,0	14,3	0,3	18,8	0,3
Pohlaví										
muži	836,7	29,6	1 419,3	50,2	35,5	1,3	7,0	0,2	10,6	0,4
ženy	625,8	23,8	1 221,4	46,4	20,8	0,8	7,3	0,3	8,2	0,3
Věková skupina										
16–24 let	355,8	32,3	555,8	50,5	24,0	2,2	.	.	.	.
25–34 let	410,7	29,7	758,7	54,9	14,7	1,1	.	.	8,6	0,6
35–44 let	340,9	27,5	572,0	46,1	8,0	0,6	.	.	.	.
45–54 let	219,3	24,3	430,3	47,7	7,0	0,8	.	.	.	.
55–64 let	103,2	16,5	243,1	38,9	.	.	.	.	.	.
65–74 let	23,9	13,8	62,7	36,1	.	.	.	.	.	.
75+	8,7	26,3	18,1	55,0	.	.	.	.	.	.

Zabezpečení osobního počítače, 2. čtvrtletí 2010

	Uživatelé internetu															
	vědí, jak je jejich počítač / počítač v jejich domácnosti zabezpečen		z toho:										nevědí, jak je jejich počítač / počítač v jejich domácnosti zabezpečen		nemají vlastní počítač / žijí v domácnosti bez počítače	
			používají antivirus		používají antispyware		používají firewall		používají spam-filtr		nepoužívají žádný nástroj					
	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]	v tis.	%[1]
Celkem 16+	3 874,7	71,0	3 549,4	65,0	1 080,9	19,8	929,5	17,0	871,0	16,0	17,2	0,3	1 246,0	22,8	334,8	6,1
Celkem 16–74 let	3 853,6	71,0	3 533,6	65,1	1 074,4	19,8	918,7	16,9	862,9	15,9	17,2	0,3	1 234,1	22,7	334,8	6,2
Pohlaví																
muži	2 233,2	79,1	2 032,9	72,0	675,9	23,9	596,4	21,1	551,4	19,5	7,1	0,3	438,3	15,5	151,3	5,4
ženy	1 641,4	62,3	1 516,6	57,6	405,0	15,4	333,0	12,6	319,6	12,1	10,1	0,4	807,7	30,7	183,5	7,0
Věková skupina																
16–24 let	876,5	79,6	802,9	72,9	269,3	24,4	201,9	18,3	202,7	18,4	.	.	150,3	13,6	74,6	6,8
25–34 let	1 038,5	75,2	944,4	68,4	289,8	21,0	249,3	18,1	230,6	16,7	.	.	253,8	18,4	88,9	6,4
35–44 let	843,4	67,9	784,1	63,1	235,5	19,0	218,3	17,6	198,9	16,0	.	.	331,7	26,7	63,8	5,1
45–54 let	607,2	67,3	555,7	61,6	169,8	18,8	173,6	19,2	141,8	15,7	.	.	248,5	27,5	47,1	5,2
55–64 let	390,0	62,4	356,3	57,0	85,9	13,7	53,5	8,6	73,8	11,8	.	.	183,7	29,4	51,3	8,2
65–74 let	98,1	56,6	90,3	52,1	24,1	13,9	22,1	12,7	15,2	8,7	.	.	66,1	38,2	9,2	5,3
75+	21,1	64,0	15,8	48,0	6,5	19,7	10,8	32,7	8,0	24,3	.	.	11,9	36,0	.	.

[1] Hodnota je procentem z celkového počtu uživatelů internetu v dané socio-demografické skupině

5) Šetření ČSÚ: Informační společnost v číslech – 2016 [29]

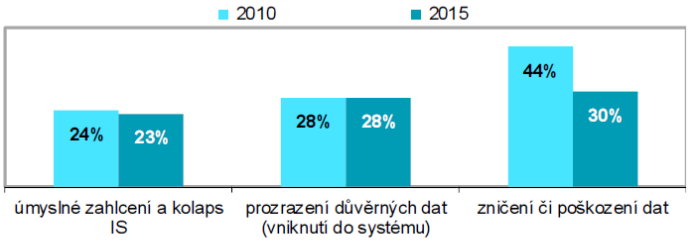
Podniky v ČR s definovanou bezpečnostní politikou informačního systému

%

	leden 2010	leden 2015
Celkem (10 a více zaměstnanců)	**21,7**	**33,4**
malé (10–49 zaměstnanců)	15,2	26,2
střední (50–249 zaměstnanců)	42,7	56,0
velké (250 a více zaměstnanců)	66,0	74,7
podle ekonomické činnosti		
Zpracovatelský průmysl	22,2	33,6
Výroba a rozvod energie, plynu a vody	25,0	39,7
Stavebnictví	12,9	23,8
Obchod, opravy a údržba mot. vozidel	27,0	39,0
Velkoobchod, kromě motor. vozidel	32,5	41,8
Maloobchod, kromě motor. vozidel	14,5	16,9
Doprava a skladování	14,0	23,0
Ubytování	13,2	33,6
Stravování a pohostinství	10,2	11,6
Činnosti cest. agentur a kanceláří	27,2	41,9
Audiovizuální činnosti; vydavatelství	35,7	53,6
Telekomunikační činnosti	42,0	53,7
Činnosti v oblasti IT	54,9	74,6
Peněžnictví a pojišťovnictví	67,1	77,6
Činnosti v oblasti nemovitostí	20,9	35,2
Profesní, vědecké a technické činn.	29,0	47,0
Administrativní a podpůrné činnosti	19,4	35,5

podíl z celkového počtu podniků v dané kategorii

Podniky, jejichž bezpečnostní politika IS pokrývá vybraná rizika; leden 2015



podíl z celkového počtu podniků

6) Šetření ČSÚ: Informační technologie v podnikatelském sektoru [30]

	Počet firem celkem	Kdo zajišťuje bezpečnost a ochranu dat		
		zaměstnanci	externí dodavatel	nikdo z uvedených /firma nevyužívá
Období konání průzkumu		**leden 2016**		
Celkem (10 a více zaměstnanců)	**38 192**	**14,0**	**63,8**	**20,5**
malé (10–49 zaměstnanců)	30 170	11,4	63,4	23,2
střední (50–249 zaměstnanců)	6 483	19,4	69,0	10,8
velké (250 a více zaměstnanců)	1 539	40,3	51,8	7,6

7) Souhlas s použitím informací – Mgr. Zuzana Duračinská (CSIRT.CZ)

Souhlas s použitím informací

poskytnutých při rozhovoru pro účely výzkumu v rámci bakalářské práce

Respondentka svým podpisem uděluje řešiteli práce souhlas se zpracováním a použitím informací získaných během rozhovoru ve společnosti CZ.NIC z.s.p.o. Souhlas platí do odvolání a je možné ho kdykoliv odvolat.

Níže podepsaný řešitel práce se zavazuje, že se získaným materiálem bude pracovat výhradně on. Získané informace budou použity ke zpracování bakalářské práce. Po přepsání rozhovoru dojde k autorizaci textu – respondentka bude mít možnost zkontrolovat a opravit uvedené údaje.

V Praze dne 23. 3. 2017

[redacted]

Adam Ostruszka
řešitel bakalářské práce
Fakulta informatiky a managementu UHK

[redacted]

Mgr. Zuzana Duračinská
specialistka na kybernetickou bezpečnost
CSIRT.CZ (CZ.NIC)

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2016/2017

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Ostruszka Adam	[redacted]	I14117

TÉMA ČESKY:

Hrozby z pohledu systémového myšlení

TÉMA ANGLICKY:

Threats from the Perspective of Systems Thinking

VEDOUCÍ PRÁCE:

doc. Ing. Hana Tomášková, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je analýza hrozeb a tvorba jejich modelu pomocí systémové dynamiky.

Osnova:
1. Obsah
2. Úvod
3. Cíl a metodika práce
4. Teoretická část
 4.1 Systémová dynamika
 4.2 Analýza hrozeb
5. Praktická část–model hrozeb
6. Analýza výsledků
7. Závěry a doporučení
8. Seznam použitých zdrojů

SEZNAM DOPORUČENÉ LITERATURY:

Gharajedaghi, Jamshid. Systems thinking: Managing chaos and complexity: A platform for designing business architecture. Elsevier, 2011.
Bureš, Vladimír. Systémové myšlení pro manažery. Professional Publishing, 2011.
Sageman, Marc. Understanding terror networks. University of Pennsylvania Press, 2004.
Hoffman, Bruce, and Fernando Reinares, eds. The Evolution of the Global Terrorist Threat: From 9/11 to Osama Bin Laden's Death. Columbia University Press, 2014.

Podpis studenta: [redacted] **Datum:** 11.10.2016

Podpis vedoucího práce: [redacted] **Datum:** 11.10.2016