MASARYKOVA UNIVERZITA
Fakulta sociálních studií
Katedra politologie

Mgr. Jakub Drmola

Kybernetická bezpečnost: systémový model protidžihádistického vigilantismu

Disertační práce

Školitel: prof. JUDr. PhDr. Miroslav Mareš, Ph.D.

Brno 2017

Čestné prohlášení

Čestně prohlašuji, že jsem disertační práci s názvem *Kybernetická bezpečnost: systémový model protidžihádistického vigilantismu* vypracoval samostatně a uvedl veškerou použitou literaturu a prameny.

V Brně dne 20. 9. 2017

Jakub Drmola

Poděkování

Za odborné vedení a pomoc v průběhu celého mého studia si v prvé řadě zaslouží velké poděkování Miroslav Mareš. Za podněty, spolupráci, kritiku, trpělivost a plamenné akademické rozepře na půdě naší fakulty i mimo ni bych chtěl poděkovat především Petře Vejvodové, Janu Hanzelkovi a Vendule Divišové. Vděk si zaslouží také všichni bývalí i současní kolegové z našeho oboru, kteří mě motivovali, rozvíjeli a společně tvořili a stále tvoří plodné prostředí.

Pronikání do konceptuálních a metodologických tajů dynamických systémů, jejich modelů a simulací by nepochybně bylo o poznání pomalejší a méně příjemné, kdyby mne při něm neprovázeli Tomáš Hubík, Niels van Rosmalen, Jonas Matheus, Tim Clancy a mnoho dalších mentorů a kolegů z UiB, EMSD a SDS. I jim všem patří můj dík.

V neposlední řadě musím poděkovat své rodině a přátelům za neutuchající podporu během studia i mimo něj a za tolik potřebná rozptýlení, bez nichž by průchod doktorským studiem nebyl možný.

Anotace

Tato disertační práce se zabývá povahou a vlivem protidžihádistického vigilantismu v kyberprostoru na džihádismem motivovaný terorismus, a to zejména z hlediska počtu útoků a množství jejich obětí. K tomuto účelu je sestaven hybridní stochastický model, který stojí na metodách Systémové dynamiky a principech mocninných zákonů. Tento model je validován na historických datech z let 2007-2016 a umožňuje i kupředu hledící simulace.

V první části práce jsou představeny hlavní teoretické koncepty, v druhé části je vysvětlen metodologický rámec a třetí část je rozdělena na popis struktury modelu a výsledky provedených simulací.

Klíčová slova: kybernetická bezpečnost, terorismus, džihádismus, vigilantismus, systémová dynamika, mocninný zákon

Annotation

Aim of this dissertation thesis is to explore the character of antijihadist vigilantism in cyberspace and the impact it has on jihadism-motivated terrorism measured by the number of attacks and the number of casualties. For this purpose, a hybrid stochastic model is built using the methods of system dynamics and principles of power laws. This model is then validated on the historical data from the period of 2007-2016 and allows for forward-looking simulations.

The first part of the thesis introduces key theoretical concepts, the second part explains the methodology used here and the third part is split into a description of the structure model and the results of the performed simulations.

Keywords: cybersecurity, terrorism, jihadism, vigilantism, system dynamics, power law

Obsah

1 Úvod ... 9

2 Cíle ... 12

3 Teorie a konceptualizace ... 14

3.1 Terorismus ... 14

3.1.1 Radikalizace ... 15

3.1.2 Typy útoků ... 17

3.2 Hacktivismus ... 21

3.3 Vigilantismus ... 23

3.3.1 Metody ... 26

3.3.2 Aktéři ... 28

3.4 Role správců digitálního obsahu ... 30

4 Metodologie ... 32

4.1 Systémová dynamika ... 32

4.1.1 Epistemologický kontext ... 32

4.1.2 Historie metody ... 35

4.1.3 Kauzalita a vlastnosti dynamických systémů ... 36

4.1.4 Vizualizace a použití systémové dynamiky ... 41

4.2 Chaos a mocninné zákony ... 55

4.3 Parametry, kompromisy a vymezení modelu ... 61

5 Související výzkum ... 64

6 Referenční vzorek teroristických útoků ... 66

7 Model protidžihádistického vigilantismu v kyberprostoru ... 72

7.1 Konceptuální a kauzální struktura ... 72

7.2 Matematická a logická struktura ... 79
7.2.1 Demografický segment ... 81
7.2.2 Radikalizační segment ... 83
7.2.3 Segment generující teroristické útoky ... 85
7.2.4 Segment generující oběti teroristických útoků ... 89
7.2.5 Segment generující viditelnost džihádismu ... 92
7.2.6 Segment soupeření v kyberprostoru ... 95
7.2.7 Vigilantistický segment ... 98
7.2.8 Segment svobody a bezpečnosti v kyberprostoru ... 101
7.3 Výsledky simulací ... 104
7.3.1 Replikace historie ... 104
7.3.2 Bez eskalace řízeného terorismu ... 106
7.3.3 Bez vigilantismu v kyberprostoru ... 110
7.3.4 Navázání na historický vývoj ... 113
7.3.5 Extrapolace vlivu vigilantismu v kyberprostoru ... 116
7.4 Návrat džihádistů ze zahraničí ... 119
8 Závěr ... 123
8.1 Zhodnocení modelu ... 123
8.2 Zhodnocení výsledků ... 125
8.3 Role vigilantismu ... 129
9 Přílohy ... 132
10 Zdroje ... 140

Seznam rovnic

Rovnice 1 – růst celkové populace 81
Rovnice 2 – změna množství sympatizantů 82
Rovnice 3 – radikalizace inspirací 83
Rovnice 4 – rozsah řízeného teroristického útoku 86
Rovnice 5 – velikost inspirovaného teroristického útoku 87
Rovnice 6 – eliminace inspirovaných teroristů 87
Rovnice 7 – kalkulace obětí inspirovaných teroristických útoků 89
Rovnice 8 – změna dopadu džihádismu na veřejnost 93
Rovnice 9 – změna výskytu džihádismu v kyberprostoru 97
Rovnice 10 – výpočet vývoje síly regulace digitálního obsahu 97
Rovnice 11 – tempo IT vzdělávání 98
Rovnice 12 – tempo aktivizace protidžihádistických vigilantistů 99
Rovnice 13 – změna vnímané hrozby v kyberprostoru 102
Rovnice 14 – změna vnímané svobody v kyberprostoru 102

Seznam tabulek

Tabulka 1 – přehled teroristických útoků zahrnutých do výzkumu 68
Tabulka 2 – vlastností džihádistických teroristických útoků utříděných dle typu 71
Tabulka 3 – statistické hodnoty pro sérii simulací v základním nastavení modelu 105
Tabulka 4 - statistické hodnoty pro sérii simulací bez eskalace 108
Tabulka 5 - statistické hodnoty pro sérii simulací bez kybervigilantismu 111
Tabulka 6 – srovnání statistických hodnot mezi sériemi prodloužených simulací 114
Tabulka 7 - statistické hodnoty pro sérii prodloužených simulací bez kybervigilantismu 117
Tabulka 8 - statistické hodnoty pro série s návratem „foreign fighters“ 121
Tabulka 9 – přehled hlavních výsledných hodnot ze všech alternativ použitých ve výzkumu 125
Tabulka 10 - přehled výsledků pro páry simulací včetně a bez kybervigilantismu 129

Seznam grafů

Graf 1 – přítok a odtok vany 43
Graf 2 – vývoj hladiny ve vaně 43
Graf 3 – vývoj hladiny čaje v hrnku 45
Graf 4 – přítok čaje do hrnku 45

Graf 5 – graf vývoje počtů všech tří typů lidí v modelu šíření nemoci 47
Graf 6 – graf vývoje velikosti toků v modelu šíření nemoci 48
Graf 7 – graf cyklické dynamiky lvů a zeber 49
Graf 8 – demonstrace průběhu mocninného zákona 57
Graf 9 – ilustrativní srovnání průběhu funkce p(x) = x^(-α) pro dvě různé hodnoty α 58
Graf 10 – graf výsledných hodnot funkce = $2.021/p$ 60
Graf 11 – průběžný graf obětí džihádistických teroristických útoků za týden během let 2007-2016 69
Graf 12 – kumulativní graf obětí džihádistických teroristických útoků během let 2007-2016 70
Graf 13 – graf simulovaného přítoku a odtoku stavu inspirovaných teroristů 88
Grafy 14 - příklady počtů obětí simulovaných teroristických útoků uvnitř modelu 91
Grafy 15 - grafy zobrazující modelovaný dopad na veřejnost produkovaný oběťmi teroristických útoků. 94
Grafy 16 – grafy zobrazující modelované vlivy na výskyt džihádistické propagandy 100
Graf 17 - histogram relativních frekvencí počtů útoků během simulací v základním nastavení modelu . 104
Graf 18 – histogram relativních frekvencí počtů obětí během simulací v základním nastavení modelu.. 105
Graf 19 – komparativní graf počtu kybervigilantistů během patnácti simulací modelu 106
Graf 20 - histogram relativních frekvencí počtů útoků během simulací bez eskalace 107
Graf 21 - histogram relativních frekvencí počtů obětí během simulací bez eskalace 108
Graf 22 - histogram relativních frekvencí počtů útoků během simulací bez kybervigilantismu 110
Graf 23 - histogram relativních frekvencí počtů obětí během simulací bez kybervigilantismu 111
Graf 24 – srovnání histogramů počtů útoků mezi modely včetně a bez kybervigilantismu 112
Graf 25 - srovnání histogramů počtů obětí mezi modely včetně a bez kybervigilantismu 112
Grafy 26 – histogramy sérií prodloužených simulací 113
Graf 27 - komparace histogramů počtů útoků u prodloužených simulací 114
Graf 28 – komparace histogramů počtů obětí u prodloužených simulací 114
Graf 29 - komparativní graf celkových počtů obětí džihádistického terorismu 115
Graf 30 - histogram počtů útoků během prodloužených simulací bez kybervigilantismu 116
Graf 31 - histogram počtů obětí během prodloužených simulací bez kybervigilantismu 117
Graf 32 – komparace histogramů útoků u prodloužených simulací z hlediska vlivu kybervigilantismu . 118
Graf 33 – komparace histogramů obětí u prodloužených simulací z hlediska vlivu kybervigilantismu .. 118
Graf 34 - komparace histogramů počtů útoků při simulacích s návratem „foreign fighters“ 120
Graf 35 - komparace histogramů počtů obětí při simulacích s návratem „foreign fighters“ 120
Graf 36 - komparativní graf celkových počtů obětí terorismu s návratem „foreign fighters“ 122
Graf 37 – průběh viditelnosti džihádismu během deseti základních prodloužených simulací 128

Seznam obrázků

Obrázek 1 – rozdělení typů teroristických útoků a útočníků na spektru podle jejich organizovanosti. 20
Obrázek 2 - přehled základních typů dynamického chování systémů 38
Obrázek 3 – jednoduchý diagram stavů a toků vany 42
Obrázek 4 – jednoduchý diagram stavů a toků modelu hrnku s čajem 44
Obrázek 5 – rozšířený diagram stavů a toků modelu hrnku s čajem 46
Obrázek 6 – diagram stavů a toků modelu šíření nemoci 46
Obrázek 7 – diagram stavů a toků modelu dynamiky predátorů a kořisti na příkladu lvů a zeber 49
Obrázek 8 – diagram stavů a toků modelu závodů ve zbrojení mezi dvěma stranami 50
Obrázek 9 – redukovaný diagram kauzálních smyček vývoje populace lvů 52
Obrázek 10 – diagram kauzálních smyček interakce lvů a zeber 53
Obrázek 11 – diagram kauzálních smyček závodů ve zbrojení mezi dvěma stranami 53
Obrázek 12 – základní diagram kauzálních smyček zpětné vazby mezi terorismem a radikalizací 72
Obrázek 13 – diagram kauzální smyček terorismu s přidanými vyrovnávajícími zpětnými vazbami 73
Obrázek 14 – smíšený kauzální diagram se stavy a toky pro eskalující terorismus 74
Obrázek 15 – smíšený diagram rozšířený o sousední stavy 74
Obrázek 16 – smíšený diagram rozšířený o zpětnou vazbu nenásilné propagandy 75
Obrázek 17 – smíšený diagram rozšířený o zpětnou vazbu cenzury digitálního obsahu 76
Obrázek 18 – finální smíšený kauzální diagram rozšířeny o zpětnou vazbu vigilantismu 77
Obrázek 19 – finální diagram kauzálních smyček 78
Obrázek 20 – celkový diagram stavů a toků, první polovina 79
Obrázek 21 – celkový diagram stavů a toků, druhá polovina 80
Obrázek 22 – diagram stavů a toků demografického segmentu modelu 81
Obrázek 23 – diagram stavů a toků radikalizačního segmentu modelu 83
Obrázek 24 – diagram stavů a toků segmentu modelu generujícího teroristické útoky 85
Obrázek 25 - diagram stavů a toků segmentu modelu generujícího oběti teroristických útoků 89
Obrázek 26 - diagram stavů a toků segmentu modelu generujícího viditelnost džihádismu 92
Obrázek 27 – diagram stavů a toků segmentu modelu zachycujícího soupeření v kyberprostoru 95
Obrázek 28 – diagram stavů a toků segmentu modelu zachycujícího vývoj vigilantistů v kyberprostoru . 98
Obrázek 29 – diagram stavů a toků segmentu modelu zachycujícího vnímání kyberprostoru 101
Obrázek 30 – diagram kauzálních smyček zaměřený na děje v kyberprostoru 103

1 Úvod

Tato práce stojí na průniku dvou dominantních bezpečnostních trendů naší doby a naší společnosti. Tím prvním je rostoucí význam kyberprostoru.[1] Ten sice nelze považovat přímo za bezpečnostní hrozbu[2] jako takovou, ale jedná se o fenomén, který zásadně a hlavně velmi rychle transformuje fungování všech aspektů našeho života. Vedle ekonomiky nebo zábavy této transformaci samozřejmě neunikly ani již existující bezpečnostní hrozby, které díky rozmachu informačních a komunikačních technologií nabraly zcela nové podoby, a to co do intenzity tak i do rozsahu. Nezadržitelným tempem je takto přetvářen například svět mezinárodní špionáže, finanční kriminality, duševního vlastnictví i ozbrojených konfliktů (Singer - Friedman 2014).

Jedním z takto zasažených fenoménů je i terorismus, který sám o sobě není nikterak nový nebo převratný, avšak našemu geopolitickému prostoru se ještě v době nedávné do značné míry vyhýbal. Na terorismus bylo snadné nahlížet jako na něco, co se nás (ať už Čechů, či Evropanů) příliš netýká, co se u nás neděje, a čeho si pouze občas povšimneme v zahraničních zprávách. I přes tragické výjimky[3] tu v zásadě panoval klid a na dřívější (a o poznání krvavější) roky plné etnicitou, separatismem či marxismem motivovaných teroristických útoků se již zapomnělo (srov. York 2015).

To se zásadně změnilo začátkem roku 2015, kdy jsme stanuli tváří v tvář inovovanému terorismu, který razantně vtrhl do Evropy i na obrazovky všech našich digitálních zařízení. Velmi

---

[1] Kyberprostor je pojem zcela klíčový a zároveň proslulý svojí nedefinovatelností. Doposud neexistuje žádná obecně uznávaná definice a konsensus mezi autory panuje vlastně jen v tom, že definovat kyberprostor je velmi obtížné. Jednou z hlavních příčin je to, že tento pojem může zahrnovat aspekty sociální, kulturní, geografické, vojenské (tzv. pátá operační doména), technické i abstraktně matematické (srov. Drmola 2014a: 63-65, Ottis - Lorents 2010, Bryant 2001, Kellerman 2016: 21-33, Kramer et al. 2009: 3-42, Scaparrotti et al. 2013: I-2).

Ambicí této práce rozhodně není ustanovit novou definitivní definici kyberprostoru a ani tento pojem nehraje centrální roli při následném kvantitativním modelování, nicméně je zapotřebí alespoň vyjasnit, v jakém smyslu je k němu přistupováno. V tomto kontextu jde především o strukturu a obsah virtuálního prostoru vznikajícího propojením počítačových sítí (primárně, ale nikoliv výhradně, internetu), který je vytvářen a neustále přetvářen aktivitou lidí v něm působících. Jedná se tedy o sdílený, nehmotný a dynamicky se vyvíjející svět. Pro účel tohoto výzkumu jsou nejdůležitějšími složkami komunikace mezi uživateli, která v kyberprostoru probíhá (přímá i nepřímá), a data, která se v kyberprostoru nacházejí (ve formě textové, audiovizuální i interaktivní).

[2] Přestože se nejedná o práci zabývající se analýzou hrozeb a rizik, v zájmu kompatibility a srozumitelnosti je zde užívaná terminologie konzistentní s dominantním chápáním těchto pojmů v rámci české bezpečnostní komunity (viz Zeman 2002: 53-66).

[3] Těmi jsou především islamistické bombové útoky v Madridu (11.3. 2004) a Londýně (7.7. 2005) a také ultrapravicový útok Anderse Breivika v Oslu (22.7. 2011).

rychle se ukázalo, že tato vlna terorismu je zcela neodlučitelně spjata s nástroji a děním v kyberprostoru. Zatímco útoky samotné jsou v zásadě totožné s těmi z let předešlých a stojí na "starých" technologiích (palné či dokonce chladné zbraně, motorová vozidla a improvizované výbušniny), takřka vše ostatní stojí na technologiích moderních a s kyberprostorem úzce provázaných. [4] Od procesu radikalizace a rekrutace, přes organizaci a plánování, až po zachycení útoku a přenesení strachu na veřejnost - to vše dnes alespoň částečně probíhá online a s mobilním telefonem v ruce.

Ruku v ruce s rostoucím významem digitálního světa a jeho vlivem na původně zcela nedigitální bezpečnostní fenomény a otázky (tj. nejen terorismus) jdou i další dva procesy. Přirozenou reakcí je zápolení o dominanci v kyberprostoru mezi aktéry. Státy, korporace, organizované skupiny i jednotlivci soutěží o kontrolu nad daty a komunikačními kanály, které jim umožňují zajistit svoji bezpečnost nebo naopak napadnout jejich nepřátele. [5] Džihádismem [6] motivovaná vlna terorismu nebyla výjimkou, a tak i proti jejich aktivitám v kyberprostoru se zvedl odpor a staly se terčem snah je odtud vystrnadit. Jako počátek (resp. razantní eskalaci) tohoto doposud trvajícího střetu o využití kyberprostoru k podpoře a šíření těchto myšlenek lze označit útok na pařížskou redakci kontroverzního satiristického magazínu *Charlie Hebdo* 7. ledna 2015 (Brooking 2015). Tento akt veřejnost šokoval a k aktivitě vyburcoval nejen bezpečnostní složky, ale také část hacktivistické scény, která se vydala cestou vigilantismu a jala se džihádismus z kyberprostoru, jenž považuje za svoji vlastní doménu, vymýtit na vlastní pěst.[7]

Krátce po eskalaci tohoto digitálního konfliktu se objevily i názory kritické a pochybovačné, které jej celý označovaly za zbytečný a naivní (Franceschi-Bicchierai 2015,

---

[4] Je třeba zdůraznit, že v žádném případě se nejedná o kyberterorismus (Drmola 2013) a tato práce se tímto stále ještě hypotetickým fenoménem ani šířeji nezabývá. Přestože kyberterorismus je v současnosti často skloňovaným pojmem, teroristé se nadále drží osvědčených kinetických útoků a doposud nedošlo k žádnému útoku v kyberprostoru, který by tento mnohdy nadužívaný koncept naplňoval.

[5] Kybernetické útoky lze třídit na tři logické typy podle modelu informační bezpečnosti, tzv. C-I-A triády: tedy útoky na důvěrnost dat (***c**onfidentiality*), celistvost dat (***i**ntegrity*) a jejich dostupnost (***a**vailability*) (Gault 2015).

[6] Džihádismus (Hamid - Dar 2016) je v tomto kontextu chápán jako širší, moderní hnutí, nevázané na jakoukoliv konkrétní organizaci, které násilnými prostředky prosazuje islamismus (tj. doktrínu, že islám má hrát centrální úlohu ve veřejném i politickém životě celé společnosti). Teologicky vychází z tzv. malého džihádu aneb džihádu mečem (*džihád bi´l-sajf*).

[7] Nejviditelněji, avšak nikoliv výlučně, se angažoval známý hacktivistický kolektiv Anonymous (velmi významnou roli samozřejmě hrála jeho frankofonní frakce), který Islámskému státu i al-Kájdě veřejně "vyhlásil válku," viz https://youtu.be/P017if-CbhU.

Krypt3ia 2015). Skepse se vztahovala především k tomu, zda takovéto dění v kyberprostoru má jakýkoliv reálný dopad na životy lidí a politické dění v reálném, hmotném světě, kde teroristické útoky probíhají. Tento střet názorů do značné míry zrcadlil dřívější události, zejména tzv. Arabské jaro z roku 2011 a proti-prezidentské protesty v Íránu v roce 2009. Zde byl také využíván kyberprostor (zejména sociální sítě Twitter a Facebook) k organizaci protestů, šíření myšlenek a k podnikání útoků na protistranu.[8] A i kolem těchto událostí vřela debata ohledně toho, jakou praktickou roli tyto prostředky vlastně sehrávají (srov. Howard 2011, Shirkey 2011, Gladwell 2010, Mourtada - Salem 2011, Srinivasan 2012, Beaumont 2011, Dewey et al. 2012, Khamis - Vaughn 2011, Morozov 2011). Jedná se tak v zásadě o analogický problém, jen v jiném kontextu.

Nacházíme se tedy v situaci, kdy je džihádismem motivovaný terorismus na vzestupu a zároveň úzce provázán s děním v kyberprostoru. Přitom nám ale unikají příčinné souvislosti a ani nevíme, jaký (pokud vůbec nějaký) má konflikt probíhající v kyberprostoru dopad na život a smrt lidí mimo něj.

[8] Je dobré zmínit, že zatímco v případě terorismu a džihádismu je na využívání internetu a sociálních médií z pochopitelných důvodů nahlíženo primárně negativně, tak v případě oněch dvou zmíněných protestních vln byly sympatie liberálního Západního světa především na straně protestujících a tyto samé komunikační a mediální prostředky byly často vyzdvihovány jako pilíře svobody a demokracie. I Anonymous se tehdy zapojili na straně subverzivních sil, tj. proti tamním režimům a rozhodně ne nijak vigilantisticky (viz Ryan 2011).

2 Cíle

Jak vyplývá ze samotného názvu práce a ze situace, kterou nastínila předchozí kapitola, hlavní ambicí této disertační práce je zjistit, jak velký vliv má protidžihádistický vigilantismus v kyberprostoru na džihádistické teroristické útoky. Kýženým cílem je dospět ke kvantitativnímu výsledku, kdy by bylo možné vyjádřit, jak by se lišily frekvence a velikost útoků za nepřítomnosti toho fenoménu (pokud by se vůbec lišily). Je na místě očekávat nejen nulový (žádný vliv), ale snad i opačný, kontraintuitivní výsledek.

Aby tento cíl mohl být naplněn, je nutné vytvořit dynamický model, který by zachycoval interakce mezi relevantními aktéry, a na kterém by bylo možné simulovat jejich vzájemné vlivy. K tomu je zde využito systémové dynamiky (angl. *system dynamics*) jakožto primárního metodologického rámce.[9] Takovýto systémový model[10] tedy musí být schopen zachytit džihádistický terorismus v dostatečné komplexitě a hlavně musí být schopen replikovat realitu, včetně oné významné eskalace od roku 2015. Jinými slovy, pokud má být model použitelný k zodpovězení hlavní výzkumné otázky, musí v prvé řadě produkovat výsledky, které přiměřeně odpovídají již proběhnuvší historii. Tvorba tohoto modelu je hlavním kreativním přínosem této práce a je jí věnována většina praktické části.

Pro tento účel jsou použity dva parametry - počet útoků a počet obětí. Ty jsou zvoleny jednak proto, že jsou hlavními logickými indikátory teroristické aktivity, a navíc jsou snadno ověřitelné a dostupné. Pro posílení validity je navíc možné srovnat výsledky i za předpokladu, že by k výše

---

[9] Softwarem použitým ke konstrukci tohoto modelu i k simulování jeho chování je Stella Professional verze 1.3.1 od společnosti isee system, Inc., https://www.iseesystems.com/store/products/stella-professional.aspx

[10] **Systém**em je obecně myšlen soubor prvků a vazeb mezi nimi. V tomto případě lze hovořit o systému džihádistického terorismu, který je tvořen všemi relevantními aktéry (teroristé, oběti, veřejnost, státní bezpečnostní složky, média, hacktivisté atd.) a interakcemi mezi nimi.

Model je manipulovatelná a zjednodušená reprezentace skutečnosti a lze jej tak považovat za idealizaci reálného systému. Dochází k záměrnému opomíjení těch částí, které jsou nepodstatné a nepotřebné vzhledem k účelu modelu, a ke zdůraznění těch klíčových. Mohou existovat na spektru od fyzických (např. model letadla nebo molekuly) až po abstraktní a matematické, což je případ této práce. Model již ze své podstaty musí realitu zjednodušovat, neboť pokud by tomu tak nebylo a byl by stejně komplexní jako realita, nijak by neusnadňoval její pochopení a neplnil by tak svůj účel.

Zatímco model imituje strukturu systému, pod pojmem **simulace** se skrývá uvedení takovéhoto modelu "do chodu" a dochází tak navíc k imitaci či reprezentaci jeho chování a procesů. To nám umožňuje zkoumat jeho chování v čase a za různých podmínek. V ideálním případě dokážeme předpovídat i budoucí chování celého systému (Novotný - Svobodová 2014: 84-85).

zmíněné eskalaci vůbec nedošlo (extrapolací vývoje do roku 2014 včetně). Vznikají tak čtyři kontrolní datové body, vůči kterým lze poměřit přesnost modelu. Vzhledem k charakteru práce je jako maximální přípustná odchylka od historických i extrapolovaných výsledků zvolena tolerance 5%.

Aby mohlo k takovému srovnání vůbec dojít, je zapotřebí sestavit i úplnou databázi teroristických útoků, které spadají do záběru výzkumu. Z hlediska časového horizontu je zvoleno období posledních deseti let, tj. 1. 1. 2007 až 31. 12. 2016. Geograficky (či snad kulturně a ideologicky) je výzkum omezen na útoky, které proběhly na území tzv. "Západu." Sestavením tohoto datového vzorku se zabývá samostatná kapitola.

Na takto validovaném modelu je pak možné prozkoumat vliv vigilantismu v kyberprostoru a kvantifikovat jej. Dále se nabízí využití takového dynamického modelu i k výhledu do budoucnosti (v tomto případě na dalších deset let) a k otestování scénářů očekávaného vývoje systému, zejména s ohledem na obávaný návrat mudžáhidů či dobrovolných zahraničních bojovníků (anglicky obvykle nazývaných obecně *foreign fighters*) ze Sýrie a Iráku po teritoriálním a vojenském kolapsu Islámského státu, který se zdá být již neodvratitelným (viz Kilcullen 2017, van Ginkel - Entenmann 2016, Winter - Clarke 2017, Lister 2016, Holmer - Shtuni 2017).

3 Teorie a konceptualizace

Zatímco pojetí většiny termínů a základních konceptů postačuje stručně objasnit v poznámkách při jednotlivých kapitolách tak, jak přirozeně vyvstávají na řadu v plynoucím textu, některé z nich jsou pro níže konstruovaný model natolik zásadní, že je potřeba se do nich zanořit hlouběji a podrobněji. Dalším důvodem je i to, že se tyto koncepty mohou mírně vymykat ze zažitého rámce politických věd a bezpečnostních studií, a tak si zaslouží více prostoru.

3.1 Terorismus

Terorismus je konceptem pro tuto práci zcela zásadním a rovněž patří k těm obtížněji definovatelným. Naštěstí již dekády trvající a intenzivní zájem ze strany akademické sféry, mezinárodních organizací i bezpečnostních složek o tento fenomén se zasloužily o to, že přestože neexistuje naprostá definiční shoda, tak v hlavních rysech se dominantní definice v zásadě překrývají (alespoň ty akademické, které jsou pro tuto práci nejdůležitější). Hlavní brzdou snah o dosažení konsensu jsou politické a právní implikace terorismu. Navíc jde o termín, který je užíván i k delegitimizaci oponentů, což de facto blokuje jakoukoliv naději na dosažení mezinárodně uznatelné a závazné definice. To, že se alespoň akademická obec v zásadě shoduje, je o to více pozoruhodné a záslužné.

Autorem, který se tomuto definičnímu problému věnoval nejvíce, je nepochybně Alex Schmid, který mimo jiné sesbíral a analyzoval přes 250 akademických, historických, vládních i mezinárodních definic terorismu (2004, 2011: 39-157). Na tomto základě předkládá definici, kterou respektuje i tato práce. Terorismus definuje jako konspirativní, demonstrativní a kalkulovanou násilnou činnost prováděnou bez morálních či etických zábran, cílící primárně na civilisty, jejímž účelem je propagandistický a psychologický dopad na veřejnost a strany konfliktu. Zároveň tak označuje i doktrínu stavějící na předpokládané účinnosti této taktiky, jež využívá strachu a politického násilí jakožto donucovacího prostředku.[11]

Tuto definici tamtéž upřesňuje a rozvíjí dalšími jedenácti body, z nichž některé stojí za vyzdvihnutí, neboť se vztahují i ke zde předkládanému výzkumu:

[11] Vlastní volný překlad z anglického originálu (Schmid 2011: 86).

- užití fyzického násilí (nebo jeho hrozba) může mít charakter jednorázových aktů (např. bombové útoky nebo přepady za pomocí palných zbraní) i vícenásobných sekvencí (únosy, držení rukojmí, útoky kombinované v čase i prostoru atd.);
- terorismus lze považovat za formu komunikace směřující jednak k publiku, vůči kterému jsou činěny požadavky i hrozby, a také k reprezentovanému segmentu populace, od kterého je poptávána podpora;
- přímé oběti terorismu nejsou tím skutečným cílem útoku, nýbrž pouze prostředkem ke generování poselství, které je dále za pomocí médií šířeno až ke konečnému publiku (či straně konfliktu), které se identifikuje buďto s utrpením obětí nebo s posláním teroristů;
- zdrojem teroristického násilí mohou být jednotlivci, malé skupiny, mezinárodní sítě či státní a státem podporovaní aktéři;
- přestože se terorismus svými metodami v mnohém podobá organizovanému zločinu, liší se především politickou motivací a společenskými důsledky;
- teroristické akty zpravidla nejsou izolované, ale naopak tvoří souvislou násilnou kampaň a právě hrozba opakování útoků vytváří atmosféru strachu, která umožňuje ovlivnění politického procesu.

Do záběru této práce tak spadají ty akty, které naplňují výše uvedené znaky a navíc je lze označit za džihádistické (viz pozn. 6). Jedná se tedy o násilnou činnost, která nerozlišuje mezi oběťmi (angl. *indiscriminate*), je prováděna s cílem zastrašit publikum či inspirovat sympatizanty, a je motivována přesvědčením, že politika i společnost mají být založeny na islámu (nejčastěji na jeho krajně konzervativní verzi, která se odkazuje k životu prvních generací muslimů, tj. na salafismu).[12]

3.1.1 Radikalizace

Při konstruování modelu tohoto typu se nelze vyhnout ani centrální roli, kterou sehrává radikalizace. Jedná se o další, dnes často skloňovaný termín, který se obtížně definuje. Existují přístupy zaměřující se na psychologii jednotlivců a na druhé straně i přístupy spíše celospolečenské

[12] Je třeba upozornit, že islamismus ani salafismus sami o sobě nijak neimplikují násilný boj, což je jeden z důvodů, proč je zde upřednostněn termín džihádismus. Někdy je možné setkat se i s obsahově analogickým termínem qutbismus, což je explicitně násilná doktrína formulovaná egyptským inspirativním myslitelem jménem Sajjid Qutb (Manne 2016, Eikmeier 2007). Jedná se ovšem o relativně málo známý termín.

a politické. Dále můžeme rozlišovat mezi radikalizací z hlediska přesvědčení a z hlediska chování (srov. Borum 2011, Neumann 2003, Sedgwick 2010, Silke 2008, Horgan 2008).

Vzhledem k tomu, že tento model pracuje na velmi agregované a stochastické úrovni, nejsou individuální psychologické pochody radikalizovaných jedinců pro tuto práci nijak zásadní.[13] Důležité je spíše celkové směřování tohoto procesu (od nezainteresovaného člověka, přes ideologického sympatizanta, až k aktivní participaci na teroristických útocích) a pak také vektory, kterými je tento proces zprostředkován. Vzhledem k zaměření této práce na kyberprostor a tamní soupeření je tu důležitá role internetu a digitálních médií jakožto prostředku radikalizace (Neumann 2013, Carter - Maher - Neuman 2014). Tato role je nyní středem pozornosti, a to nejen v souvislosti s náboženským radikalismem, ale například i ve vztahu ke krajní pravici (viz Wilkinson 2016).

Zatímco v "offline světě" má velký význam přímý kontakt s jinou radikální osobou (např. v rámci rodiny, lokální náboženské komunity nebo vězení), díky kterému může být radikalizovaná osoba náchylnější přijmout nové nahlížení na svět, kyberprostor pro tento proces skýtá jiné výhody (podle von Behr - Reding - Edwards - Gribbon 2013):

- internet vytváří více příležitostí k radikalizaci, otevírá nové komunikační kanály a nové zdroje informací, umožňuje zasáhnout větší množství lidí než lokální média;
- internet vytváří ozvěnu, která posiluje a normalizuje již existující extrémní názory, usnadňuje nalezení lidí a zdrojů sdílejících a podporujících stejné názory;[14]

---

[13] McCauley a Moskalenko (2008: 418) nabízejí užitečnou systematizaci mechanismů radikalizace. Představují pyramidový model skládající se ze dvanácti vrstev postupujících od individuální, přes skupinovou, až po masovou úroveň radikalizace. Agregovanost této práce ale nespočívá v tom, že by pracovala pouze s mechanismy masové úrovně. Naopak akceptuje a do modelu zahrnuje všechny tyto mechanismy, včetně těch na individuální úrovni, ale nijak mezi nimi nerozlišuje, ať už jde o radikalizaci skrze osobní křivdu nebo skrze kulturu mučednictví.

[14] Tento problém sociálních médií jakožto generátorů ozvěn (angl. *echo chambers*) se také netýká pouze náboženského radikalismu. Tzv. *echo chamber effect*, který vede i ke vzájemnému izolování nesouhlasících komunit, zahlušení oponující argumentů a místy až k vyhrocenému tribalismu či démonizaci, byl v kontextu kyberprostoru nepřímo postulován již před řadou let (viz např. Morozov 2011). Maximální pozornost mu ale začala být věnována až v souvislosti s vítězstvím Donalda Trumpa v prezidentských volbách USA v roce 2016, které vyvolalo kritiku zejména vůči algoritmům Facebooku, jejichž nezamýšleným důsledkem je právě takováto segregace podle ideologických dělících linií (El-Bermawy 2016, Hosangar 2016, Quattrociochi et al. 2016). Tento vývoj je v ostrém kontrastu s místy už utopickými představami o tom, jak má internet sbližovat světové komunity a budovat vzájemné porozumění. Nicméně i přesto, že se tuto vizi naplňovat příliš nedaří, místy v tomto prostředí dochází k pozoruhodným interakcím mezi znepřátelenými stranami konfliktu, viz transkript v příloze.

- internet akceleruje proces radikalizace, neboť poskytuje kontinuální a de facto ničím neomezený a nepřerušovaný přístup k poptávaným materiálům a radikálním komunitám;
- internet umožňuje, aby radikalizace probíhala z pohodlí domova, anonymně, bez ohledu na vzdálenosti mezi lidmi, státní hranice a fyzické limity, které by jim jinak bránily v kontaktu;
- internet zprostředkovává sebe-radikalizaci, kdy se člověk vlastní činností a bez přímého kontaktu (fyzického ani elektronického) s kýmkoliv jiným nezávisle zradikalizuje.

I přes tyto specifické možnosti, které kyberprostor nabízí, je důležité mít na paměti, že proces radikalizace obvykle kombinuje kontakty v obou sférách. Digitální a materiální svět jsou úzce propojené a i v tomto případě se navzájem spíše doplňují a podporují, než že by se měly nahrazovat. Tímto synergickým způsobem jsou oba radikalizační vektory zachyceny i v modelu, jejich efekt se kombinuje a působí na tu samou populaci tím stejným směrem (avšak nikoliv nutně stejnou silou).

3.1.2 Typy útoků

Klíčovým aspektem, který model zohledňuje, je míra organizovanosti teroristických útoků. Čím dál více autorů začíná rozpoznávat, že džihádistické teroristické útoky nejsou všechny stejné, naopak se od sebe velmi liší z hlediska plánování, počtu zapojených útočníků, jejich materiálního vybavení a kontaktů s dalšími aktéry. Tyto faktory pak výrazně ovlivňují výsledné počty obětí, které takový útok způsobí.

Počet kategorií, do kterých lze teroristické útoky třídit, není fixní ani ustálený, hranice mezi nimi jsou velmi mlhavé a kategorie se často překrývají. I přes tuto dosavadní neukotvenost se jedná o koncept, který tato práce pominout nemůže. Následuje přehled nejčastěji rozpoznávaných typů (vychází z Clancy 2016b, Vidio - Marone - Entemann 2017, Ellis et al. 2016, Joscelyn 2016, Callimachi 2017, Farnham - Liem 2017, Moreng 2016).

Na pomyslném vrcholu z hlediska obětí a celkového dopadu zpravidla stojí teroristické útoky, které jsou přímo plánované, organizované či řízené (angl. nejčastěji pojmenovávané jako *directed*) někým, kdo je prakticky součástí etablované teroristické organizace. Útok samotný většinou provádí tým několika lidí, z nichž alespoň část má bojovou zkušenost či prošla výcvikem se zbraněmi a trhavinami (typicky někde v jedné z konfliktních oblastí Blízkého Východu). Skupina disponuje dostatečnými finančními prostředky, které získali od organizátorů, a skrze

zprostředkované kontakty si dokáže obstarat automatické zbraně, falešné doklady atp. Udržují kontakt a svoji činnost koordinují. Tyto teroristické útoky jsou logisticky i finančně nejnáročnější, nejméně časté a bývají také nejkrvavější. Typickými příklady takovýchto řízených útoků jsou třeba ty z Bruselu 22. 3. 2016 (32 zabitých), Paříže 13. 11. 2015 (128 zabitých), nebo, zabrousíme-li více do historie, z New Yorku 11. 9. 2001 (2977 zabitých). Na druhou stranu jejich organizační náročnost a počet zapojených lidí zvyšují šanci, že plán bude odhalen a zmařen bezpečnostními složkami.

Druhou kategorií jsou takzvané útoky zprostředkované nebo virtuálně řízené (angl. se nejčastěji používá označení *enabled* a *virtual planners*). Jedná se o typ ve své podstatě nový a umožněný rozkvětem kyberprostoru. Takovýto terorista není nijak zapojen do jakékoliv teroristické organizace a ani s nikým z ní není v přímém osobním kontaktu. Nicméně podaří se mu navázat virtuální spojení[15] s někým, kdo ho navádí k provedení útoku a poskytuje mu asistenci. Tento styčný důstojník či "manažer" (*handler*) se může nacházet v libovolné zemi, zůstává od útoku izolován a svými radami (výjimečně i zprostředkováním omezené materiální asistence) se snaží zařídit co nejefektivnější útok za situace, kdy jeho "svěřenec" má nejspíše jen minimální relevantní zkušenosti, dovednosti a prostředky. Zároveň usiluje i o maximální propagandistický účinek. Jako příklady mohou posloužit třeba útok sekerou ve vlaku ve Wurzburgu 18. 7. 2016 (5 zraněných) nebo exploze v Ansbachu 24. 6. 2016 (15 zraněných).

Organizačně už naprosto oddělenou kategorií jsou útoky pouze inspirované (*inspired*) sdílenou myšlenkou a přesvědčením, v tomto případě džihádismem. Cílem je podpořit a dále šířit poselství. Nedochází již vůbec k žádné vzájemné přímé komunikaci mezi útočníky a teroristickou organizací (samozřejmě do toho nespadají různé veřejné a plošné výzvy nabádající sympatizanty

---

[15] Takovýto kontakt probíhá téměř výhradně skrze automaticky šifrované komunikační kanály, jež jsou v rostoucí míře součástí běžně dostupných mobilních aplikací (například WhatsApp, Viber, Telegram, Signal). Za normálních okolností je takto zašifrovaná komunikace (v kombinaci s adekvátně chráněným celým telefonem) nejen nezachytitelná během přípravy útoku, ale navíc zůstává nepřístupnou i po jeho vykonání. Bezpečnostní složky tak při vyšetřování přichází o cenný zdroj informací a často ani sami provozovatelé služeb a výrobci zařízení nejsou technicky schopni obsah zpráv dešifrovat (což je záměrná vlastnost celého systému). Není nijak překvapivé, že tento technologický segment čelí ostré kritice ze strany vyšetřovacích orgánů i politiků (viz Sparrow 2017, Armasu 2017).

Podobné debaty se již delší čas vedou i ohledně projektu TOR (The Onion Router), který umožňuje anonymní přístup k webovým stránkám a do tzv. Dark Web, který může mimo jiné soužit třeba i k ilegálnímu obchodu s drogami či šíření dětské pornografie. Tato zdánlivě jednoznačná situace je ovšem značně komplikována tím, že na těchto krypto-technologiích stojí například i fungování (a často i životy) investigativních novinářů nebo disidentů v represivních režimech (Zimmerman 1999, Schneier 2016).

k násilí) ani k žádné materiální, finanční nebo logistické podpoře. Inspirovat se kromě ideologie mohou i metodami a může dojít i ke vzniku malé nezávislé buňky, jež útok připravuje. Kvůli jejich izolovanosti a nezávislosti jsou tyto teroristické útoky často označovány jako díla "osamělých vlků" (*lone wolf terrorism*). Za zástupce tohoto typu lze označit třeba útok v New Yorku 23. 10. 2014 (2 zranění) a v Nice 14. 7. 2016 (85 zabitých). Často je ale obtížné, až nemožné definitivně zjistit, zda k nějakému kontaktu docházelo či nikoliv, a tak může dojít k tomu, že zprostředkovaný útok (*enabled*) je chybně identifikován jako útok osamělého vlka.

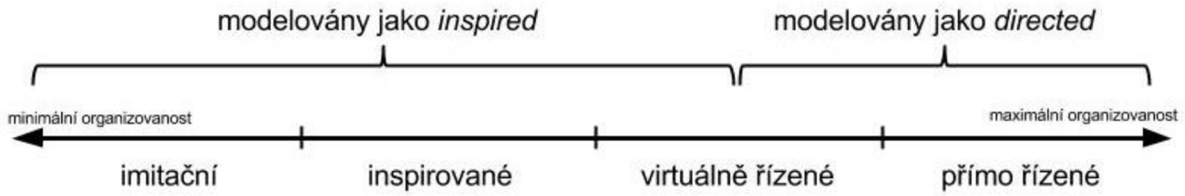
Poslední kategorií jsou teroristické útoky, které napodobují a imitují předešlé útoky spíše z psychologických než z ideologických důvodů. V anglickém diskursu se mohou objevit pod názvem *copycat* nebo *Werther terrorism*, což jsou pojmy inspirované potenciální nakažlivostí sebevražd, obzvláště pokud se jedná o široce publikované případy (např. u celebrit).[16] Podobně nakažlivé mohou být i teroristické útoky pro psychicky nestabilní jedince (skrze tzv. ideaci). Z tohoto důvodu se obvykle jedná o útoky individuální a dochází k nim krátce po jiných, silně medializovaných útocích (efekt shlukování, angl. *clustering*). V důsledku se tak tento typ nachází na pomezí psychopatologického terorismu (viz Mareš 2005). Hlavní motivací je vykonat násilný a viditelný akt, jeho ideologické zdůvodnění je až sekundární a deklarovaná příslušnost k nějakému hnutí či myšlence vyplývá z jeho momentální viditelnosti. Útočník chce ze svých vlastních vnitřních psychologických důvodů emulovat již provedené útoky, které zaujaly pozornost veřejnosti, a spíše se přidat k něčemu významnému. Politická nebo teologická zdůvodnění zapojení se do takového konfliktu nejsou rozhodující. Nejznámějším příkladem terorismu tohoto typu je útok v Orlandu 12. 6. 2016 (49 zabitých), kde útočník Omar Mateen (Sullivan - Wan 2016) vůbec nenaplňoval charakteristiky džihádisty a dokonce střídavě proklamoval loajalitu ke vzájemně znepřáteleným skupinám. Za další takovéto imitační teroristické útoky lze považovat ten v Quebecu 22. 10. 2014 (1 zabitý) nebo v Sydney 15. 12. 2014 (2 zabití).

Ve všech čtyřech případech rozhodně platí, že hranice mezi sousedícími typy jsou pružné a specifická kategorizace záleží na dostupných (obvykle neúplných) informacích a interpretaci. Je

[16] Rozpoznání tohoto efektu (pojmenovaného podle tragického protagonisty románu Utrpení mladého Werthera, který napsal Goethe v roce 1774 a údajně tím vyvolal vlnu sebevražd) a snaha o jeho minimalizaci vedli i k adopci směrnic pro média ohledně podávání zpráv o sebevraždách (Phillips 1974, Norris - Jempson - Bygrave - Thorsen 2006). Stojí tak přinejmenším za zvážení, zda by něco ekvivalentního mělo význam i pro zprávy o teroristických útocích.

obtížné jednoznačně stanovit, jak významný podíl by měli mít na útoku skuteční členové teroristické organizace, aby jej šlo označit za útok přímo řízený (*directed*) a kdy jde ještě o útok jen virtuálně řízený (*enabled*). Je obtížné jednoznačně prokázat, zda byl útočník opravdu osamělým vlkem v pravém slova smyslu (*inspired*), neboť jen těžko lze s naprostou jistotou vyloučit, že by udržoval kontakt s někým, kdo mu k útoku mohl napomoci. A už vůbec není možné jednoznačně určit, zda u útočníka sehrál hlavní roli jeho radikální islamismus, anebo jestli už byly klíčové spíše jeho psychické predispozice (*copycat*).

Vzhledem k propustnosti těchto kategorií se ve zjednodušené formě vlastně jedná o spektrum na jedné ose od největší po nejmenší organizovanost útoku. To umožňuje flexibilní rozdělení tohoto spektra dle potřeb konkrétního výzkumu. Pro účely zde prezentovaného dynamického modelu je zvoleno zjednodušené rozdělení na dvě kategorie, které spektrum dělí přibližně na poloviny. Základem jsou idealizované kategorie řízeného a inspirovaného typu. Psychologicky podmíněný werther terorismus je zahrnut do kategorie *inspired*, zatímco kategorie *enabled* je rozpuštěna do dvou s ní sousedících. Alternativně lze na toto přerozdělení nahlížet i tím způsobem, že kategorie *directed* a *inspired* jsou rozšířeny tak, aby do sebe zahrnuly i ty dvě zbývající a aby bylo spektrum pokryto celé.



Obrázek 1 – rozdělení typů teroristických útoků a útočníků na spektru podle jejich organizovanosti.

Důvody pro toto mírně asymetrické přerozdělení celého spektra a rozložení virtuálně řízených útoků do dvou sousedních kategorií namísto jeho podřazení pod *directed* plynou z rozsahu externí podpory, kterou útočníci získávají, a z účinků, jakých pak dosahují. Z pohledu modelu je dělení útoků a teroristů na *directed* a *inspired* významné hlavně kvůli jejich rozsahu a počtu obětí, přičemž ty řízené jsou typicky rozsáhlejší a s větším množstvím obětí.

Imaginární hranicí, která prochází skrze virtuální útoky, a která je pak aplikovaná v dynamickém modelu, je to, zda *handler* budoucímu útočníkovi zprostředkuje i nějaké finance, vybavení nebo kontakty využité při teroristickém útoku samotném - v tom případě lze útok

považovat za *directed*. Pokud se ovšem jedná spíše jen o rady, morální podporu a nabádání k činu, tedy nedochází ke zprostředkování ničeho jiného než informací, je útok zařazen pod *inspired*.

Tato metoda totiž nebývá vždy zcela účinná, jak demonstruje třeba případ Riaze Khana, který byl svým kontaktem z řad ISIS explicitně přemlouván, aby ke svému útoku využil automobil, čímž by napáchal maximum škod. To ale Khan odmítl a trval na použití chladných zbraní, neboť se chtěl mučedníkem stát co nejdříve a nehodlal marnit svůj čas tím, že by sháněl automobil a učil se jej řídit (Joscelyn 2016). Dalším významným faktorem je to, že jsou tímto způsobem často instruováni aspirující džihádisté, kteří by ale ve skutečnosti preferovali vycestovat do Sýrie či Iráku, aby mohli žít a bojovat tam. Kvůli zhoršující se průchodnosti hranic a rostoucímu tření mezi frakcemi uvnitř ISIS (zejména mezi místními a zahraničními bojovníky) jsou ale nabádáni k teroristickým útokům ve svých domovinách, neboť z pohledu organizace to je daleko efektivnější využití těchto lidí (Mironova - Hussein 2016, Callimachi 2017). Výsledkem jsou pak nepříliš dobře připravené a provedené útoky, jejichž účinky zpravidla nedosahují těch skutečně řízených a důkladně organizovaných.

3.2 Hacktivismus

Etymologicky i funkčně je hacktivismus spojením politického aktivismus a tzv. hackování. Jde tedy o zpravidla neoprávněné využívání počítačových systémů a sítí nebo narušování jejich chodu s cílem rozšířit ideologické poselství či podpořit nějaký politický směr.[17] Kromě této jednoduché a obecné definice je vhodné tento koncept i vymezit vůči jemu podobným (viz Denning 1999, Singer - Friedman 2014: 77-80).

Standardní politický aktivismus již dnes zcela přirozeně využívá prostředky IT a zasahuje do kyberprostoru. Oproti hacktivismu ale využívá jen běžných forem svého šíření a nedochází k žádnému úmyslnému narušení (angl. *disruption*) regulérního chodu počítačových systémů ani sítí. Může jít třeba o rozesílání informačních nebo agitačních e-mailů, provoz debatních fór, zakládání skupin na sociálních sítích, sdílení příspěvků, šíření politické reklam atp.

[17] Je záhodno upozornit, že v tomto bodě se text terminologicky mírně rozchází se českým Výkladovým slovníkem kybernetické bezpečnosti (Jirásek - Novák - Požár 2013: 40-41), který používá formu "hactivism." Tato práce ale dává přednost formě, která je již etablovaná v mezinárodním akademickém i technologickém diskursu.

Kyberterorismus (viz pozn. 4) by naopak způsobil nenávratnou fyzickou destrukci cenného zařízení nebo ztráty na lidských životech. Oproti hacktivismu tak jde o zásadně závažnější a ničivější fenomén, který s hacktivismem nelze zaměňovat, přestože sdílejí politický aspekt.

S kybernetickou kriminalitou hacktivismus do značné míry sdílí nástroje a metody. Zcela jednoznačně se ale odlišují z hlediska motivace, neboť zatímco hacktivisté jsou motivováni svým politickým přesvědčením, tak kybernetická kriminalita je páchána s vidinou vlastního prospěchu (většinou finančního obohacení). Druhým častým atributem kyberkriminality je snaha autorů tyto operace utajit, kdežto hacktivisté se snaží o maximální publicitu.[18]

Kyberšpionáž a kybersabotáže jsou doménou státních aktérů, kteří při nich rovněž usilují o největší možné utajení. Proto jsou obvykle v gesci zpravodajských služeb nebo armád. S hacktivismem zde ale dochází k mírnému překryvu v oblasti informační války a propagandistických operací, neboť využívají stejné prostředky a jednoznačně identifikovat útočníka v kyberprostoru je extrémně obtížné.[19] Situaci dále komplikuje existence hackerských skupin bojujících za zájmy konkrétního státu, přičemž ale není jasné, zda se jedná o patriotické hackery (někdy se používá i označení kybermilice, *cybermilitia*), najatou skupinu hackerů (tzv. kyberžoldnéřství, *cybermercenaries*), nebo o státní složku, která se za hacktivisty jen vydává.[20]

Historické kořeny hacktivismu lze hledat na přelomu osmdesátých a devadesátých let minulého století (Denning 2015). Dominantní myšlenkou, která tehdy hacktivisty motivovala k vyjadřování svého přesvědčení skrze narušování chodu napadaných sítí, byl odpor vůči jadernému

---

[18] Z pohledu této terminologie nehraje žádnou roli legalita (respektive ilegalita) obou aktivit. Přestože i některé formy hacktivismu mohou být (a často i jsou) za hranicí lokálních zákonů, nejsou v kontextu debat a prací zabývajících se těmito fenomény z technologického, politického, kulturního nebo strategického hlediska považovány za kyberkriminalitu (*cybercrime*) v pravém slova smyslu. I když to někdy může být matoucí, bývá tento termín vyhrazen pro finančně motivované kyberútoky, zatímco ty politicky motivované jsou označovány jako hacktivismus, a to ať už k porušení zákona dojde či nikoliv. Vzhledem k tomu, že se nejedná o právnický ani kriminalistický výzkum, je tento výklad použit i zde.

[19] Problém identifikace útočníků a atribuce útoků je v současnosti jedním z nejpalčivějších problémů v kontextu soupeření mezi státy v kyberprostoru. Kyberprostor nerespektuje politické ani geografické hranice a útok může přijít odkudkoliv kamkoliv. Útočníci často zůstávají anonymní a neidentifikovaní. Kdo za útokem vlastně stál, můžeme dedukovat jen s omezenou pravděpodobností na základě úvah o tom, komu takový útok vůbec prospěl, kdo má prostředky k jeho provedení a jaké jsme nalezli technické indicie. Neschopnost komukoliv jednoznačně přiřknout zodpovědnost za kybernetický útok zásadně omezuje nejen možnost trestně stíhat pachatele ale i schopnost států navzájem se odstrašovat od excesivní špionáže a destruktivních sabotáží (Poznansky - Perkoski 2016, Lindsay 2015, Hare 2012, Schneier 2015).

[20] Jako příklady těchto skupin, u nichž není zcela jasný jejich vztah se státem, jehož zájmy v kyberprostoru prosazují, lze uvést třeba proruské FancyBear (https://fancybear.net/) a CyberBerkut (https://cyber-berkut.org/), Iranian Cyber Army nebo Syrian Electronic Army.

zbrojení a pokračujícím jaderným testům. Do historie hacktivismu se později zapsala také válka v Kosovu, přičemž se jednak protestovalo proti jejímu samotnému zahájení a později se stránky institucí USA staly cílem vlny útoků z Číny, když omylem došlo k vybombardování čínské ambasády v Bělehradu. Postupem času přibývalo agendy i skupin. Za přelomový moment pro hacktivismus, jeho sílu a viditelnost lze považovat rok 2008 a zahájení "Project Chanology," což byla rozsáhlá operace hnutí Anonymous proti Scientologické církvi.[21]

V politickém, mediálním i kulturním povědomí se Anonymous definitivně ukotvili během let 2010 a 2011, kdy se postavili za WikiLeaks a PirateBay, proti dohodě ACTA a zapojili se do Arabského jara na straně protirežimních demonstrantů. V současnosti existují stovky hacktivistických skupin, které v kyberprostoru bojují za nejrůznější politické směry. Za tímto rozmachem stojí částečně tehdejší relativní úspěch a popularita Anonymous a částečně neustále se zrychlující horizontální i vertikální proliferace informačních technologií. Díky tomu se každým rokem zvyšuje množství potenciálně napadnutelných cílů, roste jejich společenský význam a viditelnost, a zároveň přibývá i lidí, kteří jsou schopní a motivovaní se zapojit. Proto je dnes již obtížné vůbec najít nějaký ideologický nebo politický konflikt (neřkuli rovnou vojenský), který by se obešel bez paralelních projevů hacktivismu v kyberprostoru (Coleman 2015, Denning 2015).

3.3 Vigilantismus

Vigilantisté[22] jsou lidé, kteří vynucují dodržování státních zákonů a společenských norem (resp. dodržování jejich vlastní interpretace těchto zákonů a norem), a přitom nejsou součástí jakékoliv státní instituce či složky tímto se zabývající a postrádají jakoukoliv oficiální autoritu. Jedná se vlastně o fenomén, kdy lidé takzvaně "berou zákon do vlastních rukou." V případě probíhajícího konfliktu mezi státem a nějakými subverzními protirežimními nebo kriminálními elementy lze vigilantisty považovat za součást represivních sil. Na druhou stranu uvnitř silných právních a liberálně demokratických států se vigilantisté snadno mohou dostat do sporu se státními složkami, pokud narušují jejich monopol na užití síly. Typickými příklady jsou různé domobrany,

[21] Project Chanology (kombinace jména serveru 4Chan.org a slova Scientology) původně vznikl jako reakce na agresivní snahy Scientologické církve o cenzurování svých uniklých interních materiálů na internetu. Anonymous jej zahájili dnes již ikonickým výhružným videem "zpráva pro scientologii": https://www.youtube.com/watch?v=JCbKv9yiLiQ

[22] Slovo má původ ve španělském *vigilante*, tedy "hlídač" nebo "strážný."

sousedské hlídky a neregulované milice. Dle kontextu na ně může být nahlíženo jako na hrdiny, na zločince, na obránce ideálů i jejich rozvratitele (Newby 2012, Juliano 2012).

Koncept vigilantismu použitý v tomto textu vychází z práce Lese Johnstona (1996). Ten identifikoval šest charakteristik, které podle něj vigilantismus jasně definují:

- Vigilantismus je organizovaný, plánovaný, systematický a předem připravovaný. Tedy nejedná se o jednorázové spontánní akty.
- Vigilantismus je dobrovolně vykonáván civilisty a nikoliv členy jakýchkoliv bezpečnostních složek. Sporné ovšem je, zda by sem spadala třeba činnost policistů mimo službu, nicméně v kontextu této práce se nejedná o problematický bod.
- Vigilantismus není nijak posvěcen ani podporován státní mocí. Je autonomní, stojí "vedle" státní moci a jedná se iniciativu zespod.
- Vigilantismus využívá síly a hrozby použití síly. Tímto je zpravidla myšleno fyzické násilí, ale v obecnější rovině si pod silou lze představit i jiné formy újmy. Taková činnost tak může a nemusí být ilegální dle zákonů země, kde k ní dochází.
- Vigilantismus vzniká jako reakce na vnímané porušování institucionalizovaných a společenských norem, tj. všeobecně přijímaného pořádku. Jimi prosazovaná verze spravedlnosti tedy nemusí být nutně v naprosté shodě s platnými zákony, zejména pokud jsou považovány za nespravedlivé nebo naopak příliš laxní.
- Vigilantismus má za cíl takovémuto porušování norem zamezit a zajistit v oblasti bezpečnost (subjektivně pojatou) pro vlastní participanty i pro ostatní.[23]

Transponováním vigilantismu do kyberprostoru nebo kombinací vigilantismu s hacktivismem vzniká veskrze nezvukomalebný novotvar zvaný kybervigilantismus (angl. *cybervigilantism*, někdy se lze setkat i s termínem *digilantism,* viz Nhan - Huey - Broll 2017). Na tento koncept lze tedy nahlížet buďto jako na specifickou podmnožinu hacktivismu, kdy oním politickým cílem konkrétních hacktivistů je potlačení aktérů porušujících akceptované normy, nebo jako na vigilantismus na internetu, přičemž klasické fyzické násilí je nahrazeno různými kybernetickými

[23] Vedle reálných historických případů je pozoruhodné, jak frekventovaný je tento koncept ve fiktivních příbězích. Mnoho populárních hrdinů naplňuje valnou většinu Johnstonových atributů – až ikonicky sem spadá třeba Batman. Za povšimnutí stojí i to, že jasnou ukázkou vigilantismu je také hrdina filmu *V for Vendetta*, od kterého hacktivistické hnutí Anonymous převzalo dnes již tolik rozpoznatelnou černobílou masku jako svůj primární symbol.

útoky (viz Smallridge - Wagner - Crowl 2016). Oba úhly pohledu v důsledku vedou k totožnému konceptu, takže fakticky není důvod mezi nimi rozlišovat. I když se jedná koncept zcela nový a v diskursu nepříliš rozšířený, nelze jej považovat za nadmíru problematický (v porovnání s jinými koncepty z této oblasti). I tak je ale vhodné blíže si jej stručně vymezit.

Podle Trottiera (2016) je pojícím prvkem kybervigilantismu snaha identifikovat a zviditelnit normy porušující aktéry a přitáhnout na ně jimi rozhodně nechtěnou pozornost. K tomuto vymezení je ale zapotřebí přidat i útoky, které mají naopak za cíl minimalizovat jejich viditelnost a znemožnit jim jejich zamýšlené aktivity v kyberprostoru, což je obzvláště relevantní pro tuto práci.[24]

Dále rozhodně není nutné, aby tímto způsobem byly potlačovány výlučně ty transgrese proti vnímaným normám, ke kterým by docházelo v kyberprostoru. Kybervigilantismus sice využívá výlučně prostředí a nástrojů kyberprostoru, ale může takto napadat cíle i aktivity mimo něj.

Musí být splněna podmínka, že dochází k nějaké reálné újmě (nebo je alespoň použita výhrůžka). Místo fyzického násilí se tak může jednat třeba o finanční ztráty, poškození reputace, ztrátu soukromí, veřejnou dehonestaci, nebo zveřejnění ilegální činnosti a identity pachatelů v kombinaci s případným nátlakem na bezpečnostní složky, aby na tomto základě jednaly. Obvykle dochází k této újmě v návaznosti na nějaký kyberútok narušující chod počítačových systémů a sítí, nicméně někdy mohou být využity i legitimní (a zároveň legální) prostředky.

Typickými příklady, během kterých obvykle nedochází k napadení žádných systémů, jsou snahy o využití rozsáhlých sociálních sítí a znalostí a kontaktů širokého spektra lidí k odhalení, deanonymizaci a identifikaci lidí na základě velmi omezených informací (například videa, které zachycuje zavrženíhodný čin). Časté jsou také kampaně, při nichž jsou lidé považováni za legitimní cíl masového obtěžování, jsou šířeny informace o jejich předpokládaném prohřešku a i jejich rodina nebo zaměstnavatel jsou zahlcováni dehonestujícími zprávami. Častým spouštěčem těchto masových zahanbovacích tažení (tzv. *name & shame*) je třeba týrání zvířat nebo obvinění ze sexuálního obtěžování, neřkuli pedofilie. Vzhledem k davové mentalitě a rychlosti šíření může

[24] Dalším a poměrně okrajovým výkladem kybervigilantismu je tzv. *hack-back*, tedy například situace, kdy by nějaká firma zjistila, že je na ni prováděn kyberútok (třeba ve formě průmyslové špionáže), a přistoupila by k přímému protiútoku proti zdroji napadení (Woodall 2014).

jít o extrémně škodlivý fenomén, zejména pokud se původní obvinění ukáže býti falešné (Cheong - Gong 2010, Wade 2014, Nhan - Huey - Broll 2017).[25]

V rámci této práce jsou ze spektra kybervigilantismu samozřejmě vybrány pouze jeho protidžihádistické projevy. Mimo to se lze setkat zejména s kybervigilantismem cíleným proti již výše zmíněnému týrání zvířat, sexuálním zločinům, dětské pornografii, korupci a ultrapravicovým uskupením.[26] Na závěr této kapitoly se také hodí explicitně zmínit, že není-li v textu specifikováno jinak, vigilantismem (tedy i bez v dnešní době až příliš všudypřítomné předpony kyber-) je v modelu i jeho analýze vždy míněna jeho forma mířená proti džihádistům a probíhající v kyberprostoru.

3.3.1 Metody

Jak bylo uvedeno výše, zlomovým bodem pro protidžihádistický vigilantismus v kyberprostoru byl útok na redakci *Charlie Hebdo* v Paříži na počátku roku 2015. Tento teroristický útok mobilizoval část hacktivistů, kteří se rozhodli proti džihádismu (v tomto období reprezentovaným především Islámským státem) aktivně vystoupit. V nejobecnější rovině se jedná o potlačování a narušování veškerých aktivit, ke kterým džihádisté kyberprostor využívají. Kromě demonstrace síly a odporu byly tyto snahy zdůvodňovány i zamezením komunikace mezi teroristy a jejich existujícími nebo potenciálními přívrženci (Brooking 2015, Reisinger 2015).

Pravděpodobně nejviditelnější a v prvních fázích také nejrozsáhlejší aktivitou byly útoky na webové stránky, které byly vyhodnoceny jako s džihádismem nějak propojené. Jednalo se například o stránky oslavující teroristické útoky, obhajující nebo propagující džihádismus, obsahující instrukce a návody[27] nebo považované za rekrutační kanál. Tohoto bylo a je možné dosáhnout v zásadě třemi způsoby. Prvním a nejpřímočařejším je zahlcení hostitelského serveru obrovským množstvím dat, aby je nestíhal vyhodnocovat a reagovat na ně a stal se tak pro ostatní

---

[25] V kritickém kontextu se tyto aktivity přirovnávají k honům na čarodějnice, angl. *witch hunts* (Gaskill 2016).

[26] Proti některým jiným zločinům jsou takovéto útoky naopak neporovnatelně vzácnější (až nevídané). Například digitální pirátství a porušování autorských práv není mezi hacktivisty obvykle považováno za cokoliv závadného a nevidí důvod jej jakkoliv potírat.

[27] Efektivita diseminace takovýchto návodů (jak vyrobit bombu, jak provést útok, jak zůstat v utajení atp.) a schopnost lidí něco takového se naučit pouze skrze digitální instrukce nejspíše daleko zaostává za přímými tréninkovými metodami i za radikalizačním potenciálem kyberprostoru (viz Kenney 2010). I to může být jeden z důvodů, proč jsou inspirované útoky relativně často neúspěšné.

uživatele nedostupným, tedy DDoS útok (*Distributed Denial of Service*). Jde o ukázkový útok hrubou silou v kyberprostoru, který není nijak náročný a může se do něj zapojit prakticky každý (případně si tento útok lze i zaplatit jako službu). Druhým způsobem, technicky o poznání složitějším, je tzv. *defacement,* kdy útočník dočasně převezme kontrolu nad obsahem webové stránky a může jej změnit - typicky třeba za výhrůžné, urážlivé nebo zesměšňující poselství, které se po útoku návštěvníkům stránky zobrazí namísto očekávaného obsahu. Poslední variantou je vyvíjení nátlaku na provozovatele serveru, který takovéto stránce poskytuje webhosting (někdy i zcela nevědomky), přičemž cílem je, aby jim byly vypovězeny služby. Dlužno dodat, že tyto útoky sice patří k těm nejviditelnějším, ale v zásadě mají všechny jen velmi krátkodobý účinek (nejvýše v horizontu dnů).[28]

Analogicky lze nahlížet na útoky mířené proti džihádistickým účtům na sociálních médiích (Facebook, Twitter, YouTube, Instagram atp., viz Berger - Morgan 2015). Proti nim sice prakticky nelze provádět DDoS útoky, ale je možné se pokusit převzít nad nimi kontrolu (například odhalením nebo prolomením hesla) nebo se zasadit o jejich zablokování ze strany provozovatelů těchto platforem. Takto zablokované účty bývají zpravidla odstraněny definitivně, nicméně je snadné nahradit je účty novými. Dochází tím ale ke snížení jejich propojenosti a sledovanosti, takže přeci jen přinejmenším dočasně klesá jejich dopad na potenciální publikum. Hacktivisty

[28] Jak už to u vigilantismu bývá, dochází i k zasažení nezamýšlených cílů. Například pokud zcela jiné a s terorismem nijak nesouvisející stránky nevědomky sdílí webhostingový server se zamýšleným cílem, na nějž je zaměřen DDoS útok, stanou se také nedostupnými. Dalším zdrojem chyb je jazyková neznalost kombinovaná s přehnanou horlivostí v řadách hacktivistů, což vede k napadání čehokoliv, kde je obsah psán arabským písmem a podle obrázků vypadá alespoň vágně relevantně. Takto se mohou terčem stát i stránky, které svým ideologickým zaměřením spíše stojí proti džihádismu reprezentovanému Islámským státem – například šíitské, súfistické nebo kurdské.

V tomto stejném období lze také zaznamenat velké množství útoků směřující opačným směrem, jejichž původci jsou naopak hacktivisté džihádismus podporující (většinou pod hlavičkou tzv. *CyberCaliphate*, viz Murphy 2015). Nejčastěji dochází k napadání webových stránek a zaměňování jejich obsahu za ikonografii ISIS, zprávy oslavující jejich útoky nebo vyhrožování útoky novými. Na druhou stranu, zatímco takto šířené poselství je ideologicky jednoznačné, jejich volba cílů je z velké části oportunistická a obvykle vůbec nezáleží na tom, jaký je původní obsah takto napadeného serveru, ale zda obsahuje nějakou zranitelnost, kterou lze k útoku využít (například stránky japonského instruktora tance, australské firmy dodávající beton, nebo firmy ve Walesu, která vyrábí laminátové podlahy, viz Cuthbertson 2016). Dochází ale i k závažnějším pro-džihádistickým kyberútokům, kdy může dojít k úniku utajovaných informací (Constine 2015).

přivlastněné účty jsou používány ke stejným účelům jako analogicky napadené webové stránky, tj. k zesměšňování, zastrašování nebo odrazování přívrženců napadeného účtu.[29]

Speciální a vzácnou formou kybervigilantismu je navazování přímé komunikace s kontakty z řad Islámského státu, které se snaží potenciální přívržence přesvědčit k cestě na území samozvaného chalífátu a často jim s ní i logisticky nebo finančně pomoci. Hacktivisté se mohou vydávat za takovéto zájemce, přičemž jejich cílem je přinejmenším mrhat časem těchto rekrutérů, tuto činnost jim znechutit a v ideálním případě z nich i vylákat nějaký finanční obnos. Takováto forma vigilantismu ale může vyvolat nežádoucí reakci ze strany bezpečnostních složek, obzvláště dojde-li k nějaké finanční transakci, které jsou často sledované (Peritz 2015).

Poslední formou je infiltrace uzavřených džihádistických skupin a monitorování jejich komunikace v kyberprostoru. Cílem je nalézt další komunikační kanály k napadení, odhalit identity skrývající se pod jednotlivými pseudonymy a zachytit plány budoucích útoků. Takto získané informace mohou být postoupeny bezpečnostním složkám, které by na ně měly reagovat, k čemuž již údajně několikrát došlo (Cuthbertson 2015, Parkin 2016).[30]

Kontroverzním aspektem je ale možná interference mezi aktivitami hacktivistů a bezpečnostních složek. Neustálé a nekoordinované útoky na webové stránky, sociální účty a komunikační kanály džihádistů a jejich podporovatelů mohou v jistých případech i zmařit probíhající policejní nebo zpravodajské operace. Je trvajícím a nerozřešeným dilematem, zda je lepší tyto komunikační kanály blokovat a omezovat jejich účinek anebo zda je výhodnější je využít ke sběru dat o džihádistech samotných a jejich plánech (Greenmeier 2015, Berger - Morgan 2015: 52-61).

3.3.2 Aktéři

---

[29] Asi nejznámějším případem byla vlna útoků v polovině roku 2016, kdy byly nabourány stovky džihádistických účtu a jejich ultrakonzervativní obsah byl nahrazen obrázky a odkazy se silně homosexuální a homoerotickou tématikou (Bridgeman 2016, Segall 2016).

[30] Pozoruhodným fenoménem v tomto kontextu je tzv. *crowdsourcing*, aneb využívání anonymního davu dobrovolníků, v tomto případě k analýze fotek a videí, které sami džihádisté publikují v rámci svých propagandistických snah. Lidé z notoricky známého a nechvalně proslulého fóra 4chan tímto způsobem odhalili umístění zobrazených tréninkových táborů v Sýrii, jejichž souřadnice pak zprostředkovaně předali silám Ruské federace, které je posléze vybombardovali. Zda k tomu ale opravdu došlo na základě poskytnutých informací, anebo šlo jen o shodu okolností, zůstává samozřejmě nepotvrzené (Ferréol 2016, Steinblatt 2016).

Přestože přímo model samotný nijak nerozlišuje mezi těmito jednotlivými protidžihádistickými vigilantistickými entitami, hodí se jejich spektrum stručně ilustrovat na jednotlivých aktérech, kteří se na této činnosti podílejí. Tím nejznámějším jménem je nepochybně Anonymous, nicméně nejedná se v žádném případě o jednolitou a centrálně řízenou organizaci. Anonymous je spíše jakousi „značkou“, pod kterou může vystupovat kdokoliv, kdo se k ní přihlásí. Přidruženi pod ikonickou hlavičkou této “adhokracie” se protidžihádističtí hacktivisté zaměřují především na boj v rámci sociálních médií, hlavně skrze napadání, nahlašování a blokování desítek tisíc propagandistických účtů, k čemuž využívají i anonymní dobrovolníky. Efektivita těchto aktivit bývá někdy rozporována, jednak kvůli tomu, že takto komplikují monitorování těchto účtů a navíc ne vždy je takové nahlášení opodstatněné. Jejich nejznámějšími představiteli jsou “TorReaper” a “WauchulaGhost,” ale celkově se na této činnosti pravidelně podílejí desítky až stovky lidí. Jejich pohled na situaci je takový, že touto činností brzdí radikalizaci a rozšiřování řad přívrženců džihádismu. Berou na vědomí ilegalitu svého počínání, nicméně podle nich selhávají samy společnosti, které tyto sociální platformy provozují, a tak je to na nich[31] (Segall 2016, Cottee 2015, Gilbert 2016, Varagur 2016).

Známou vigilantistickou skupinou, která se od Anonymous zcela odtrhla a distancovala v květnu 2015, je *Ghost Security Group*. V jejím čele stojí “DigitaShadow” a čítá zhruba dvacet členů. Vedle napadání a blokování sociálních účtů a webových stránek se tato skupina specializuje hlavně na výše zmíněnou infiltraci džihádistických komunikačních kanálů, sběr informací a jejich analýzu. V případě potřeby tyto informace předávají bezpečnostním složkám, což již údajně mělo vést ke zmaření několika plánovaných útoků. Přestože tato skupina s Anonymous a s ostatními hacktivisty v zásadě sdílí motivaci a cíle, kvůli odlišným metodám se často dostávají do sporů a navzájem se ostře kritizují. *Ghost Security Group* je kritizována za to, že záměrně nechává radikální obsah online, zatímco oni sami kritizují Anonymous za to, že se pletou do cesty jejich snahám zastavit chystané teroristické útoky[32] (Smith 2015, Russon 2015, Segall 2015).

---

[31] “If the social networks were doing enough, we wouldn’t be on there doing what we’re doing. Sometimes you have to stand up for what you believe in. If you want change, you have to make that change. Even if it means doing something illegal.” - WauchulaGhost (Segall 2016)

[32] "When it comes to terrorist attacks, one of the big worries is that you could take down forums and cost someone their lives. Anonymous has a habit of shooting in every direction and asking questions later." - DigitaShadow (Smith 2015)

Asi nejznámějším vigilantistickým hackerem vůbec je “Jester”. Ten je aktivní od roku 2009 a proslavil se primárně jako silně pro-americký a patriotický hacker typu osamělého vlka. Jeho skutečná identita není známa, ale podle jeho vlastních vyjádření je bývalým vojákem a i přes svoji ilegální činnost udržuje alespoň zprostředkované kontakty s americkou zpravodajskou komunitou. Kromě velkého patriotismu a projevované podpory ozbrojeným silám USA je znám také svým velmi aktivním profilem a vystupováním na sociálních sítích, rozhovory s médii a velmi nekulantní kritikou všeho, co se mu znelíbí, kam spadá i mnoho jiných hacktivistických skupin. Obzvláště na účet Anonymous se vyjadřuje velmi nevybíravě a konzistentně kriticky (viz Jester 2012, 2014).

V kyberprostoru napadá obecně kohokoliv, koho on sám sezná býti “nepřítelem USA,” a tam spadají mimo jiné i džihádisté. Jeho obecnou strategií je nabourávat provoz většiny džihádistických komunikačních platforem, a tím docílit koncentrace jejich uživatelů na menší počet lépe sledovatelných serverů a fór (Jester 2015). K dalším obvyklým cílům, proti kterým vystupuje, patří nejčastěji Rusko (Jester 2017), Korejská Lidově Demokratická Republika a podobné režimy, které vnímá jako nepřátelské vůči zájmům USA, a například server WikiLeaks, čímž se ještě více odlišuje od většiny hacktivistické scény. Svůj vigilantistický boj proti džihádismu v kyberprostoru však odůvodňuje prakticky stejně jako ostatní - zaplňuje mezeru, kterou vnímá v nedostatečném boji proti radikalizaci online[33] (Pagliery 2015, Kimery 2014, OConnor 2012).

3.4 Role správců digitálního obsahu

Tak jak s postupem času narůstá význam kyberprostoru pro aktivity džihádistů i v boji proti nim, stále větší pozornost je věnována i platformám, které jsou k tomuto účelu využívány. Zejména provozovatelé sociálních sítí a médií (zejména Google, Facebook a Twitter) čelí ostré kritice za to, že takto mimo jiné umožňují propagaci násilné ideologie a radikalizaci čím dál většího počtu lidí. Jak bylo uvedeno výše, toto vnímané selhání často tvoří základní motivaci pro vigilantismus. Kromě hacktivistů se podobně kriticky ozývá část veřejnosti i mnoho politiků, kteří rovněž požadují efektivnější regulaci a mnohem aktivnější přístup (viz Toor 2015, Bagot 2017, Cain - Gonzalez 2017).

---

[33] "I realized something needed to be done about online radicalization and 'grooming' of wannabe jihadis, and we didn't have mechanisms to deal with it. I decided to start disrupting them. … I answer to my conscience, and to God. That's about it. I think my actions speak loudly enough of my principles and doctrine." - Jester (Pagliery 2015)

I přes relativně intenzivní a již několik let trvající tlak dochází ke změnám jen velmi pomalu. Kromě toho, že se tyto společnosti logicky snaží maximalizovat množství svých uživatelů a tak nejsou implicitně zrovna nakloněny jejich blokování, jedná se zároveň o zásadní technologickou a regulatorní výzvu. Prvním problémem je samotný ohromný objem dat, kterým se tyto společnosti musí probrat a není možné jej prověřit ještě před tím, než je zveřejněn. Musí tedy jednat až reaktivně a obsah (anglicky obvykle *content*) odstraňovat až poté, co byl nějakou dobu volně dostupný. Samotný proces vyhodnocování závadnosti obsahu je sice částečně automatizován, ale konečné vyhodnocení zpravidla provádí člověk, tudíž vždy bude pomalejší než zakládání nových účtů a nahrávání nového obsahu.[34]

Druhým zásadním problémem je praktická nenalezitelnost hranice mezí tím, co by mělo a nemělo být blokováno, resp. cenzurováno. Všechny firmy nalézající se v tomto postavení neustále čelí tomuto problému a marně usilují o nalezení jasné dělící linie, přičemž čelí kritice z obou stran. Při zpřísňování pravidel regulujících obsah sociálních médií totiž vždy dojde i nezamýšleným vedlejším škodám. Mezi časté oběti patří třeba kanály, které džihádisty satirizují nebo o nich podávají zprávy, případně plní edukační funkci. Situaci komplikuje značná nejasnost a nejednotnost pravidel. Například Facebook užívá neveřejný systém, který se skládá z osmi specifikovaných chráněných kategorií (např. sexuální orientace nebo etnicita), nechráněných kategorií (např. zaměstnání nebo věk) a kvazichráněných kategorií (ty vznikají kombinacemi předchozích), podle nichž jeho cenzoři vyhodnocují obsah. To vše dále zhoršují regionální a národní rozdíly, neboť co je tolerované v jedné zemi, může být ilegální v zemi jiné (Angwin - Grassegger 2017, Karanicolas - Mendel 2016: 53-66, Magid 2017).

Je tedy pochopitelné, že tyto společnosti v této věci postupují velmi pomalu, neboť s každým přehmatem přicházejí o další zákazníky (a tím i o finance) a jsou obviňovány z nekompetentní plošné cenzury. Přitom jakmile jsou učiněny nějaké konkrétní kroky, které džihádisty v kyberprostoru negativně postihnou, je představitelům těchto firem vyhrožováno smrtí (Kosoff 2016). Zároveň je ale pochopitelné i to, že veřejnosti toto tempo přijde neúnosně pomalé, neboť o problému se hovoří již řadu let a komplexní řešení je stále v nedohlednu.[35]

---

[34] Pro ilustraci: každou minutu je na YouTube nahráno přes 400 hodin nových videí (Harris 2017).

[35] Nejnovější deradikalizační iniciativou v tomto směru je snaha automaticky přesměrovávat uživatele vyhledávající džihádistická videa na YouTube k obsahu, který vyvrací jejich narativu (Farmer 2017).

4 Metodologie

4.1 Systémová dynamika[36]

4.1.1 Epistemologický kontext

Pilířem systémové dynamiky jakožto metody a vlastně i celé této práce je veskrze pozitivistické nahlížení na svět, včetně jeho sociálních aspektů. Cílem je v podstatě imitovat úspěch přírodních věd skrze aplikaci numerických metod i na komplexní sociální systémy, které tradičním přímočarým přístupům založeným na experimentech odolávají. Při analýze těchto systémů staví především na nástrojích matematické analýzy (konkrétně na diferenciálním a integrálním počtu, aneb souhrnně kalkulus) a principech zpětné vazby.[37]

Komplexní systémy jsou takové, které vykazují vlastnosti a chování, které přímo nevyplývají z jejich dílčích elementů. Vysoké množství prvků a jejich složité interakce generují tzv. emergentní chování nebo vlastnosti, které zcela zásadně a hlavně kvalitativně mění povahu celého systému a jejichž původ není zřejmý. Typickým příkladem je třeba termitiště, jehož složitý ventilační systém nijak přímočaře nevyplývá z individuálních termitů. Sociální systémy jsou pak ty, které se skládají primárně z lidí (případně sociálních zvířat) a interakcí mezi nimi.[38]

Problémem většiny sociálních věd (včetně politologie a bezpečnostních studií) je to, že na rozdíl od přírodních věd pracují prakticky výhradně jen s komplexními sociálními systémy. Kromě obrovského množství špatně přístupných proměnných plynoucích z komplexity se pak musí potýkat i s velmi omezenými experimentálními možnostmi. Tato omezení plynou nejen ze

---

[36] Méně podrobným a jednodušším představením této metodologie se zbýval i již vydaný článek, viz Drmola 2014b.

[37] Zpětnou vazbou je obecně myšlen proces, kdy systém reaguje na nějaké podmínky a zároveň tím ovlivňuje jejich budoucí stav. Tradičním příkladem pro vysvětlení tohoto konceptu je obyčejný termostat. Ten reaguje na okolní teplotu tím, že sepne topení, čímž dojde k postupnému zvyšování teploty, dokud nedosáhne nastavené hladiny a v ten moment se přestane topit. Pokud se teplota opět vychýlí, termostat znovu zareaguje. V přírodě lze poukázat třeba na schopnost slunečnice otáčet se za sluncem. Celou evoluci skrze přirozený výběr lze vlastně vnímat jako jednu velkou zpětnou vazbu. Zpětnou vazbu lze najít i mezi voliči a politiky nebo mezi stranami válečného konfliktu.

[38] Vedle komplexních sociálních systémů lze také vymezit komplexní adaptivní systémy. Ty se vyznačují schopností reagovat na změny podmínek změnou vnitřní struktury a vlastního chování. Mezi nimi lze rozlišit adaptivní systémy přirozené (tj. nezávislé na lidské existenci), lidské a umělé, přičemž ty umělé jsou vždy výtvorem lidí a lze je dále dělit na hmotné a nehmotné. V důsledku se ale nehmotné umělé komplexní adaptivní systémy v zásadě překrývají s komplexními sociálními systémy, takže alespoň v rámci této práce je není nutné pečlivě rozlišovat (Cioffi-Revilla 2014: 7-12).

zřejmých etických důvodů spojených s experimentováním na lidech, ale i z nemožnosti kontrolovat proměnné, a vůbec replikovat zkoumané procesy. Jinými slovy, zatímco fyzici mohou bez obav a opakovaně urychlovat a rozbíjet atomy, aby zjistili, z čeho se skládají, není možné mnohokrát opakovat občanskou válku a zkoušet, jakým způsobem je nejlepší ji ukončit.[39]

Jako odpověď na tento zádrhel se postupem času prosadila široká rodina metod, která se kolektivně označuje jako komputativní sociální věda (angl. *computational social science*). Jak již název napovídá, její rozvoj je úzce spjat s proliferací výpočetní techniky, která umožňuje analyzovat systémy v dostatečné komplexitě. Uvnitř této široké disciplíny je možné nalézt čtyři oblasti, které fungují samostatně i synergisticky a interdisciplinárně. Těmi jsou automatická extrakce informací (aneb *data mining*), analýza sítí, analýza komplexity a simulace (Cioffi-Revilla 2014: 12-17).

Systémová dynamika se řadí právě mezi metody schopné simulovat modely (viz pozn. 10) komplexních sociálních systémů, a tak do jisté míry suplovat experimentální omezení sociálních věd obecně a bezpečnostních studií především.[40] Nemůžeme-li tedy experimentovat se skutečnými válečnými konflikty, můžeme experimentovat na jejich simulacích (za předpokladu, že je dokážeme zachytit způsobem, který umožňuje je simulovat, to jest skrze matematické rovnice a logické operace). Mezi další výhody simulací patří schopnost explicitní a formální kodifikace teorií, schopnost pracovat s daleko větším množstvím proměnných než zvládne pouhá výzkumníkova mysl, testování možných způsobů řešení problémů a dopadů zamýšlených zásahů do systémů (jinými slovy *policy analysis*). V zásadě jde o stejné důvody, kvůli kterým simulace využívají i disciplíny přírodních věd - od biologie po astrofyziku.

Vypovídací hodnota takovýchto simulací je samozřejmě přímo závislá na kvalitě modelu, tedy jak moc je simulovaný model komplexního sociálního systému svojí strukturou a chováním

---

[39] V některých případech se tento problém daří překonat pomocí statistických metod, které umožňují odhalit souvislosti i tam, kde nedokážeme provádět vlastní experimenty a ani neznáme všechny příčinné souvislosti uvnitř zkoumaného systému. Nutným předpokladem je ale dostatečně vysoké množství podobných případů a dostatečné nízký počet zkoumaných proměnných. Bohužel zejména v oblasti bezpečnostních otázek často platí pravý opak – případů je málo a proměnných mnoho.

[40] Přestože patří k těm rozšířenějším, systémová dynamika rozhodně není jedinou metodou schopnou simulovat modely komplexních sociálních systémů v rámci komputativních sociálních věd. Další populární metodou je například tzv. modelování agentů (*Agent-Based Modelling*), které na rozdíl od systémové dynamiky operuje na nižší, méně agregované úrovni a zaměřuje se na interakce mezi individuálními prvky uvnitř systému.

podobný své reálné předloze. Dalším omezením může být technologická náročnost, neboť s rostoucí komplexitou simulace rostou i požadavky na výpočetní sílu.

Druhým možným úhlem, ze kterého lze na systémovou dynamiku nahlížet, je skrze koncept zpětných vazeb a jejich zakomponování do analýzy sociálních systémů. Zpětné vazby jsou jedním z klíčových stavebních prvků, které zvyšují komplexitu systémů, zanášejí do nich kontraintuitivní nelinearity[41] a dávají vzniknout emergentnímu chování. Vývoj myšlení ve smyslu zpětných vazeb mezi jednotlivými prvky daného systému ve své knize velice pečlivě sleduje Richardson (1991). Přestože i mezi sociálně-vědními autory se v omezené míře tento koncept implicitně objevoval již před 20. stoletím (za zmínku nepochybně stojí *Bohatství národů* od Adama Smithe, Malthusova *Esej o principu populace*, nebo Marxova dialektika), jeho skutečné kořeny je nutné hledat spíše v přírodních vědách a především v rozvoji aplikované termodynamiky a elektrotechniky. Teprve během poválečného období byly z těchto disciplín přeneseny formalizované poznatky o významu a fungování zpětných vazeb do sociálních věd.

Richardson (1991: 92-94) rozlišuje šest historických myšlenkových směrů, z nichž nakonec vykrystalizovaly metody a přístupy stavějící na zpětných vazbách při snaze lépe pochopit naši sociální realitu: ekonometrii, inženýrství, logiku, biologii (homeostatickou a matematickou) a sociální vědy samotné. První proud označuje jako "kybernetický"[42] a kromě toho, že je o něco starší, vyznačuje se především svým zaměřením na zpětnou vazbu v řízení procesů uvnitř systémů

---

[41] Jsou také klíčovým prvkem takzvaných "zákeřných problémů" (angl. *wicked problems*, viz Rittel - Webber 1973), tedy společenských problémů, které jsou v čase proměnlivé, setrvalé a často bez precedentů, špatně definovatelné, bez jednoznačné příčiny, nemají žádné jasné správné řešení ani omezený počet možných zvolitelných řešení, případná řešení nelze předem zkoušet a navíc mohou celý problém ještě zhoršit. Terorismus nepochybně patří mezi takovéto zákeřné problémy.

Poslední zmíněná vlastnost systémů se někdy označuje jako "odolnost vůči politice" (*policy resistance*), kdy snaha o ovlivnění chování celého systému žádoucím směrem může být systémem absorbována a zatlumena anebo dokonce může dojít ke zcela opačné a kontraproduktivní reakci, kdy se systém vychýlí nežádoucím směrem. Krásně to ve své knize Sterman (2000: 5-6) demonstruje na rumunské snaze o zvýšení porodnosti v 60. letech 20. století. Až drakonický plošný zákaz potratů i antikoncepce byl po krátkém nárůstu zcela samovolně neutralizován a během pouhých čtyř let porodnost klesla k původním hodnotám, zatímco prudce vzrostla rizikovost těhotenství.

[42] Zde je třeba zdůraznit, že tato "kybernetika" má v tomto smyslu jen pramálo společného s dnešní populární předponou "kyber-," kterou užívá i tato práce. Zatímco dnes toto slovo často značí propojenost s virtuálním světem informačních technologií a digitálních dat, původní význam kybernetiky (ze starořeckého slova pro kormidelníka) leží právě ve studiu a kontrole komplexních systémů se zpětnou vazbou.

a organismů (v tomto kontextu především lidí). Zpětná vazba je z tohoto pohledu informace, která reguluje budoucí i právě probíhající chování organismu či stroje.

Proud, ke kterému řadí systémovou dynamiku, pojmenoval jako "servomechanistický." Ten se naopak zaměřuje na dynamiku chování celých systémů a analyzuje je na vyšším stupni abstrakce. Studuje, jak se navzájem ovlivňují jednotlivé části společnosti. Díky svým více technickým kořenům má také blíže k tvorbě formálních matematických modelů a simulací.

4.1.2 Historie metody

Je poměrně nezvyklé, aby se zrod celé metodologie vázal k jediné osobě, ale v případě systémové dynamiky tomu tak nepochybně je. Za jednoznačného "otce" je všemi považován nedávno zesnulý Jay Wright Forrester, který ke konci Druhé světové války působil na *Massachusetts Institute of Technology* a zabýval se primárně elektroinženýrstvím a vývojem raných počítačových subsystémů, zejména v oblasti ukládání dat. Znalosti zde nabyté pak přenesl do oblasti ekonomie, managementu a podnikového řízení, když na základě svých praktických zkušeností vydal článek a později i knihu nesoucí název *Industrial Dynamics* (Forrester 1961). Zkombinoval zde poznatky z fungování elektronických systémů (včetně důležitosti zpětných vazeb) spolu s pokrokem v informačních technologiích, které již dokázaly simulovat a analyzovat komplexní systémy a procesy uvnitř nich. Forrester ve své knize položil základy také pro způsoby formálního značení modelů a terminologii jejich jednotlivých prvků. Není pouhou shodou okolností, že první diagramy zkoumaných systémů připomínaly spíše nákresy elektrických obvodů.

Po této první aplikaci následovaly brzy další, zabývající se například fungováním měst a jejich populací (viz Forrester 1969). Nejvíce pozornosti přitáhla kniha *Meze růstu* (*Limits to Growth*), kterou v roce 1972 vydal think-tank zvaný Římský klub. Tato kniha využila systémové dynamiky k simulaci a analýze celé planety a lidstva jakožto jediného systému. Důraz byl kladen na ekonomický a populační růst, který vede k vyčerpávání přírodních zdrojů a kapacit. Nejkontroverznějším aspektem celé práce byly predikce o očekávaném kolapsu celého systému někdy během druhé poloviny 21. století.

V následujících dekádách se spektrum aplikací systémové dynamiky vytrvale rozrůstalo a kromě ekonomie a demografie se prosadila zejména v přírodních vědách a studiu ekosystémů, jejich rovnováhy a adaptací (viz Ford 1999, Moxnes 2000). Za hlavní průkopníky nasazení této

metody v oblasti bližší politickým vědám a bezpečnostním studiím lze považovat Dietera Rulloffa a Nazli Choucri, kteří nezávisle na sobě v sedmdesátých letech začali vytvářet modely a simulace ozbrojených konfliktů (Cioffi-Revilla 2014: 249-251). Čím dál větší roli hrála i pokračující proliferace osobních počítačů, neboť tyto modely není možné simulovat bez nich - jejich narůstající dostupnost zpřístupnila systémovou dynamiku mnohem většímu množství lidí. Zatímco v počátcích, za dob hluboké studené války, se ke strojům schopným těchto simulací dostali jen vybraní jednotlivci v rámci univerzit nebo státních výzkumných institucí, dnes s nimi může pracovat naprosto kdokoliv, kdo je tomu ochoten věnovat čas a úsilí.

4.1.3 Kauzalita a vlastnosti dynamických systémů

Při modelování systémů lze identifikovat jisté základní principy (viz Forrester 1968). Tím snad nejdůležitějším je co nejjasnější definování uzavřeného systému, který má být modelován. Vzhledem k tomu, že systém je obecně cokoliv, co se skládá z nějakých prvků, které mezi sebou interagují, lze za systém považovat prakticky cokoliv. Systémy navíc existují na mnoha úrovních a všechny systémy se hierarchicky skládají z mnoha menších subsystémů. Pokud bychom na stát nahlíželi jako na systém, lze identifikovat mnoho subsystémů - města, rodiny, firmy, jednotlivce. Zároveň je stát součástí mezinárodního supersystému. Pro jakoukoliv smysluplnou a prakticky uskutečnitelnou analýzu je ale nutné si určit úroveň, na které má probíhat. Chceme-li simulovat fungování státu v mezinárodním společenství, nemůžeme se v modelu nořit až na úroveň rodinných vztahů. I kdyby se nám takto odlišné úrovně podařilo zachytit, model by byl příliš nepřehledný a neplnil by svůj účel.

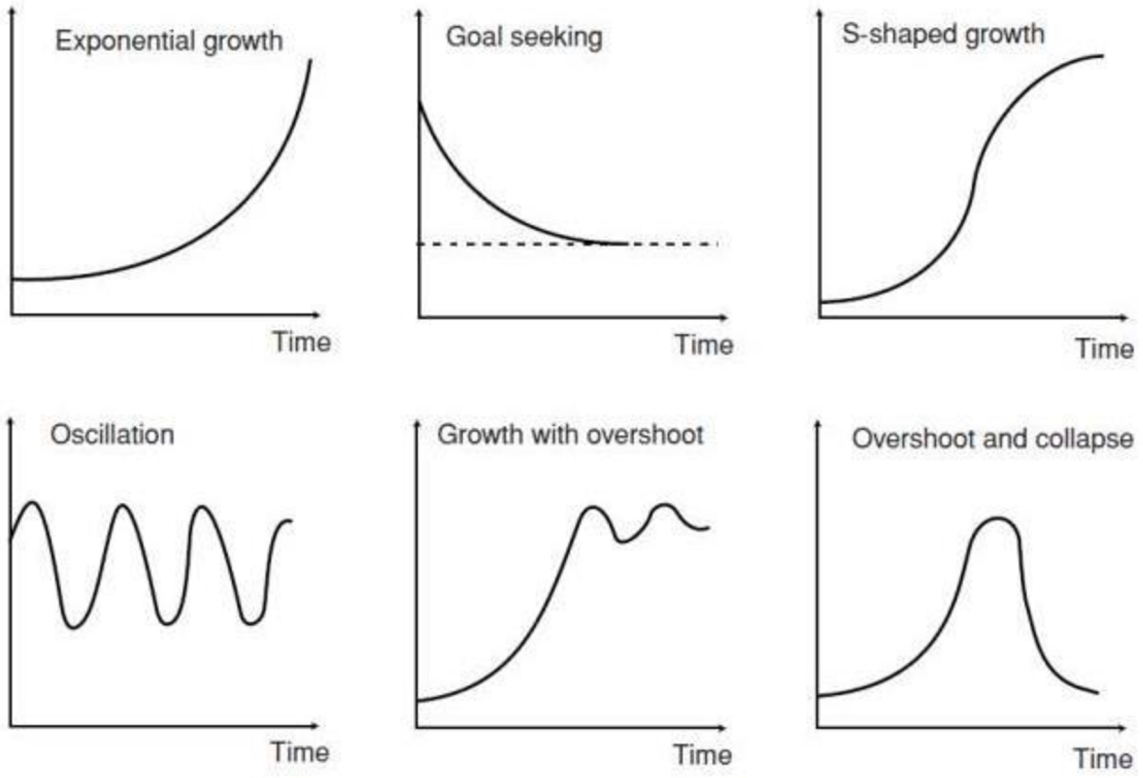
Kromě toho je zapotřebí ohraničit model i z hlediska kauzality. Cílem je zkoumat chování systému, který je produktem jeho vnitřní struktury (endogenní), nikoliv vnějších vlivů (exogenní). Proto do něj musí být zahrnuty všechny relevantní prvky, které na něj působí. Zároveň je žádoucí, aby obsahoval právě a jenom ty relevantní prvky a žádné zbytečné, které se na zkoumaném chování nijak znatelně nepodepisují. Vzniká tak uzavřený model (či systém), ve kterém nechybí žádný důležitý prvek, který by ovlivňoval jeho chování a ani žádný nepodstatný nepřebývá. Kombinací obou těchto faktorů by měla v ideálním případě být definována uzavřená kauzální hranice (*boundary*), která odděluje důležité vnitřní prvky zkoumaného systému od těch nedůležitých externích (Richardson 1991: 296-299).

Optimální zvolení této hranice je vždy velmi komplikované a zcela v režii autora modelu. V materiálním a snad do ještě větší míry i v sociálním světě totiž platí úsloví, že "vše souvisí se vším." Prakticky je velmi obtížné vůbec nalézt nějaký skutečný systém, který by byl opravdu zcela uzavřen a izolován od jakýchkoliv vnějších vlivů. I mezi sociálními systémy vždy proudí alespoň informace, a tak i při nejlepší vůli bychom uzavřený sociální systém mohli hledat jedině snad někde u dosud neobjeveného kmene v amazonském pralese. Bohužel i takovýto kmen (pokud vůbec ještě nějaký takový existuje) by byl vystaven vlivům od zbytku civilizace, například skrze změny klimatu. Proudění informací zastavit možná lze, ale proudění vzduchu nikoliv. Hypoteticky bychom se mohli vrátit daleko do historie, kdy o sobě jednotlivá civilizační centra ještě nevěděla, a vzájemné vlivy zprostředkované skrze sdílené globální životní prostředí prohlásit za zanedbatelné.

Cílem tvůrce modelu tedy není najít skutečně uzavřený systém (neboť to nelze), ale nastavit kauzální hranici kolem zvoleného systému tak, jak je to optimální vzhledem k zaměření a účelu, pro jaký daný model vzniká. Bude-li se snažit zachytit třeba dynamiku systému občanské války v Sýrii z hlediska soupeření jednotlivých znepřátelených stran, bylo by kontraproduktivní do modelu zahrnout i tamní antické kulturní dědictví, neboť přestože nějaké vzájemné působení nepochybně existuje, bude natolik slabé, že se jej oproti zkomplikování a znepřehlednění modelu nejspíše vůbec nevyplatí modelovat. V praxi tak vzniká neustálý boj mezi snahou udržet model co nejjednodušší a nutkáním přiblížit se co nejblíže skutečnosti.

Pomineme-li modely fyzických systémů (například motoru), u nichž je hledání této hranice zpravidla jednodušší, bývá hlavním vodítkem účel budovaného modelu. Model může sloužit jako preskriptivní předloha k výstavbě skutečného systému, deskriptivní pomůcka k lepšímu pochopení fungování systému, k analýze systému a odhalení příčin problematického chování, nebo jako prediktivní nástroj. Účel modelu ale nelze zaměňovat s účelem systému. U sociálních systémů a živých organismů bývá nejčastějším účelem zachování sebe sama. Tento vágní účel však lze zpravidla rozdrobit na mnoho podúčelů pro jednotlivé subsystémy, přičemž protichůdné účely bývají jednou z častých příčin problematického chování (Meadows 2008: 12-17). Vezmeme-li třeba stát jako jeden systém, jehož účelem je zachování vlastní suverenity a integrity, jeho subsystémy (např. jednotlivá ministerstva) jsou mnohdy v rozporu. U neživých a nevědomých systémů, které nebyly vytvořeny člověkem, se jasný účel hledá těžko. Účel spalovacího motoru je měnit chemickou energii na kinetickou, ale jaký je účel třeba sopky nebo sluneční soustavy?

Schopnost jednotlivých (sub)systémů naplňovat svůj účel je zprostředkována již zmíněnou zpětnovazební strukturou, kdy dochází k reakci na rozdíl mezi pozorovaným aktuálním stavem nějaké proměnné a její žádoucí hodnotou. Velikost tohoto rozdílu a rychlost reakce na její změnu je základním stavebním kamenem dynamických systémů. Vzájemné interakce mnoha takovýchto zpětných vazeb (s různými žádoucími stavy proměnných, různým zpožděním a různou silou reakce) vnáší do systému nelinearity. Ty mohou simultánně tlumit i posilovat vliv změn v různých místech systému, čímž se, pokud neznáme jeho vnitřní strukturu, chování systému stává takřka nepředvídatelným.



Obrázek 2 - přehled základních typů dynamického chování systémů

John Sterman (2000: 22 a 108) ve své knize představuje šest základních typů dynamického chování systémů v čase a shrnuje deset hlavních faktorů, jejichž kombinace toto komplexní chování způsobují:

- **Dynamičnost**: systémy vždy procházejí změnou a neustále se vyvíjejí. Jejich tempo ale není univerzální ani stálé. To, co bylo budováno v průběhu mnoha let, se může zhroutit během vteřin.

- **Propojenost**: v systémech nic neprobíhá v izolaci. Vše je propojené, vše má své důsledky a příčiny. Není možné změnit jednu část systému, aniž by se to projevilo i někde jinde.
- **Zpětné vazby**: změny ovlivňují podmínky, kterými byly původně vyvolány. Naše snahy ovlivnit svět reagují na jeho stav, čímž vytváříme stav nový, na který opět musíme reagovat.
- **Nelineárnost**: reakce často není úměrná akci. Velké snahy mohou mít jen zanedbatelnou odezvu a naopak zdánlivě nepodstatné faktory mohou mít dramatický dopad (takzvaný efekt motýlích křídel).
- **Závislost na historii**: možné budoucí směřování systému je omezené jeho minulostí (*path dependence*). Minulost nelze změnit ani vymazat, a tak je nutné žít s pozitivními i negativními dopady dřívějších akcí a rozhodnutí. To je třeba mít na paměti obzvlášť v případě nezvratných kroků, ať už jde o vykácení lesa nebo vyhlášení války.
- **Sebeorganizovanost**: chování systému vzniká spontánně z jeho vnitřní struktury. Interakce jednotlivých subsystémů ho tvaruje do finální podoby i bez vnějších zásahů nebo explicitně stanoveného cíle.
- **Adaptace**: systémy reagují na svoje prostředí a přizpůsobují se. Význam jednotlivých prvků se v čase může měnit. Lidé a komplexní sociální systémy se učí ze svých zkušeností. Ne vždy je ale taková adaptace ku prospěchu.
- **Kontraintuitivnost**: příčiny mohou být od svých následků velmi vzdálené v čase i prostoru. Lidé však intuitivně vyhledávají bezprostředně blízké příčiny, případně zaměňují příčiny se symptomy. Systémy jsou příliš složité, než aby je člověk mohl intuitivně uchopit.
- **Odolnost vůči politice**: snahy o vyřešení problému nebo změnu chování systému jsou mnohdy marné a vedou k nezamýšleným či opačným důsledkům.
- **Přechodnost**: rozdílné časové horizonty protichůdných zpětných vazeb způsobují, že okamžitý efekt může být zcela odlišný od dlouhodobého dopadu. Zdánlivě fungující řešení problému může nakonec vyústit v daleko závažnější zhoršení situace. Stejně tak optimální řešení s sebou může nést dočasné zhoršení.

Podobný přehled ve své knize uvádí i Donella Meadows (2008: 111-141), která se však spíše než na vnitřní strukturální příčiny dynamického chování systémů zaměřuje na jejich výsledné

vnější problematické projevy, které označuje jako systémové pasti. I přesto mezi oběma autory dochází k jistému překryvu:

- **Odolnost vůči politice**: neschopnost individuálních aktérů ovlivnit chování systému jimi preferovaným je podle Meadows způsobeno především jejich protichůdnými zájmy. Řešením může být sladění nebo redefinování důležitějších společných cílů.
- **Tragédie obecní pastviny** (*the tragedy of the commons*): je situace, kdy je nějaký omezený zdroj (například společná pastvina) sdílen větším množstvím aktérů. Ti, pokud chtějí maximalizovat svůj užitek, jsou nastavením systému motivování k vyčerpávání zdroje, neboť negativní důsledky se rozkládají mezi všechny aktéry. Důsledkem je rychlá degradace a konečné vyčerpání zdroje, neboť zpětná vazba je příliš slabá. Tyto pasti lze často nalézt v oblastech energetické a environmentální bezpečnosti.
- **Skluz k nižším výkonům**: pokud se plánované nebo očekávané výkony váží k těm minulým, může po prvotním poklesu dojít k nastartování zpětné vazby, která vede k trvajícímu propadu.
- **Eskalace**: je opačnou situací než skluz. Je-li cílem překonat nějakou hodnotu, která rovněž zpětně reaguje růstem, dochází k eskalující zpětné vazbě. Klasickým příkladem je bezpečnostní dilema a závody ve zbrojení, kdy státy reagují na zvyšování kapacit svých konkurentů vlastním zbrojením, což zpětně motivuje jejich konkurenty k ještě intenzivnějšímu zbrojení.
- **Úspěch úspěšným**: tato past vzniká, když je důsledkem úspěchu větší šance na budoucí úspěch, zatímco neúspěch budoucí šance snižuje. Dochází tak k rostoucí nerovnováze mezi aktéry v systému. To můžeme pozorovat primárně v prostředí ekonomickém, viz takzvané rozevírání nůžek mezi bohatými a chudými, nebo zneužívání monopolního postavení na trhu. Podobnou dynamiku můžeme pozorovat i během ozbrojených konfliktů, kdy vítězství v bitvě zvyšuje šanci na vítězství i v následující bitvě, neboť poražená strana zpravidla utrpí větší ztráty.
- **Přesun břemene** (*shifting the burden to the intervenor*): je důsledkem snah o zlepšení projevů systému skrze ovlivňování symptomů namísto jejich strukturálních příčin. Vzniká tak závislost na takovéto asistenci, kdy ukončení podpory vede k opětovnému a možná i ještě horšímu propadu. Jako příklad může posloužit kritika zahraniční humanitární pomoci, nebo hypotetické řešení globálního oteplování skrze geoinženýrství.

- **Obcházení pravidel**: pokud pravidla, kterými se systém má řídit, neodpovídají zájmům jednotlivých aktérů uvnitř něj, budou se je snažit obcházet, aniž by došlo k jejich přímému porušení. Meadows jako příklad uvádí snahu vládních institucí nebo univerzit všelijak realokovat a zbavit se získaných finančních prostředků, protože jinak by jich příště dostaly o to méně.
- **Špatné cíle**: tato past úzce souvisí s obcházením pravidel a často se obě vyskytují paralelně. Špatné cíle bývají příčinou špatných pravidel, která se pak aktéři snaží obcházet.

4.1.4 Vizualizace a použití systémové dynamiky

Kromě simulací samotných jsou hlavním výstupem systémové dynamiky diagramy, které charakterizují strukturu modelovaných systémů. Kromě toho, že jde o užitečné grafické znázornění, je tím usnadněna i samotná tvorba modelu, neboť autor není odkázán jen na sepisování abstraktních rovnic a může svůj model rovnou vidět a manipulovat s ním. Aby bylo možné model libovolného systému takto reprezentovat, musí existovat jasná formální pravidla, jak zachytit jednotlivé aspekty systémů. Přestože od prvních Forresterových modelů prošla svým vývojem, dnes jsou již zcela ustálená a homogenní a pouze se mírně odlišují dle použitého modelovacího programu (srov. Mildeová – Vojtko et al. 2008, Pospíšil 2009, Radzicki – Taylor 1997, Sterman 2000: 41-77, Meadows 2008: 27-34, Cioffi-Revilla 2014: 256-257).

Systémová dynamika ve svých modelech rozlišuje tři typy proměnných: stavovou, tokovou a okamžitou. Čtvrtým prvkem jsou pak spoje mezi nimi. Stavové proměnné (*stock*) jsou jádrem systémových modelů a zachycují ty veličiny, u kterých může docházet k postupné akumulaci v čase a zároveň si zachovávají svoji hodnotu i pokud dojde k jeho imaginárnímu zastavení. Stavy jsou ty proměnné, které představují např. množství lidí, peněz, materiálu, strojů a tak dále.

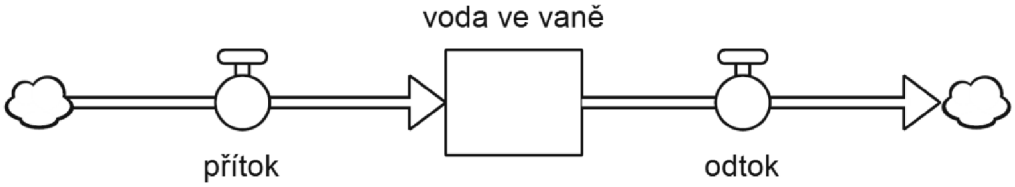
Toky (*flow*) mění hodnoty stavů. Ve vztahu ke konkrétnímu stavu lze rozlišovat odtoky a přítoky, přičemž odtok z jednoho stavu může být přítokem do jiného. Velikost tokové proměnné tak vyjadřuje rychlost změny (*rate*) stavu za jednotku času.[43]

---

[43] Obojí lze zachytit matematickými rovnicemi, na kterých pak běží simulace. Hodnotu stavu S v čase t lze vyjádřit jako integrál rozdílu přítoků I a odtoků O přičtený k počátečnímu stavu v čase t_0, tedy: $S_t = \int_{t_0}^{t}(I_t - O_t)dt + S_{t_0}$. Analogicky lze diferenciální rovnicí vyjádřit okamžitou rychlost změny stavu $d(S)/dt = I_t - O_t$ a hodnotu stavu v dalším časovém intervalu jako $S_t = S_{t-dt} + (I_t - O_t)dt$.

Proměnné s okamžitou hodnotou plní povětšinou pomocné funkce a zprostředkovávají zpětné vazby nebo zastupují konstanty. Lze na ně nahlížet i jako na speciální typ stavových proměnných, jejichž hladina se mění buď rychleji, než jaké je časové rozlišení modelu, anebo se naopak mění mnohem pomaleji, než jaký je horizont simulace a v tom případě se jedná o konstanty. Diagram stavů a toků (*Stock and Flow Diagram*, zkráceně SFD) tvoří názornou mapu modelu a zároveň je primárním pracovním prostředím systémové dynamiky.

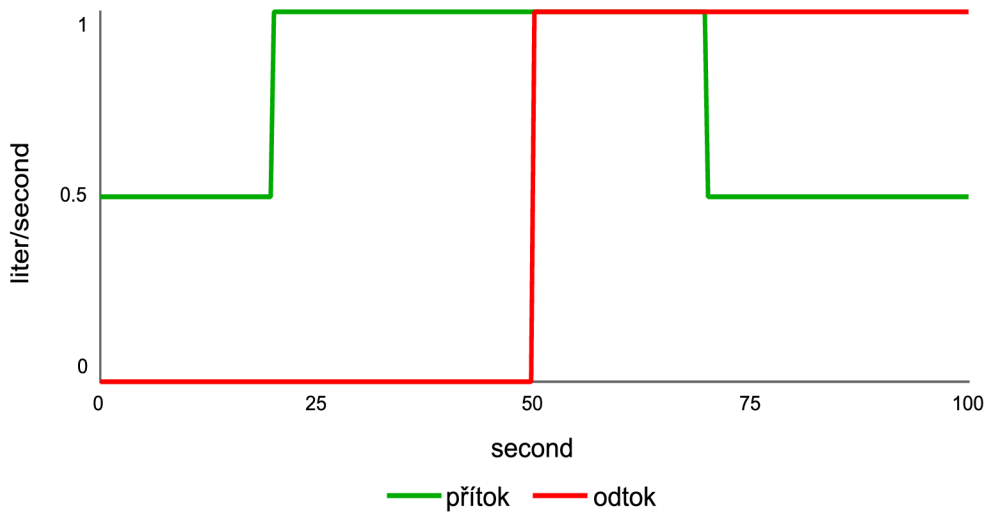
Tato terminologie přímo vybízí k častému užívání názorných příkladů s prouděním vody, kde stavy jsou reprezentovány nádobami a toky potrubím.[44] Ani tato práce nebude výjimkou.



Obrázek 3 – jednoduchý diagram stavů a toků vany

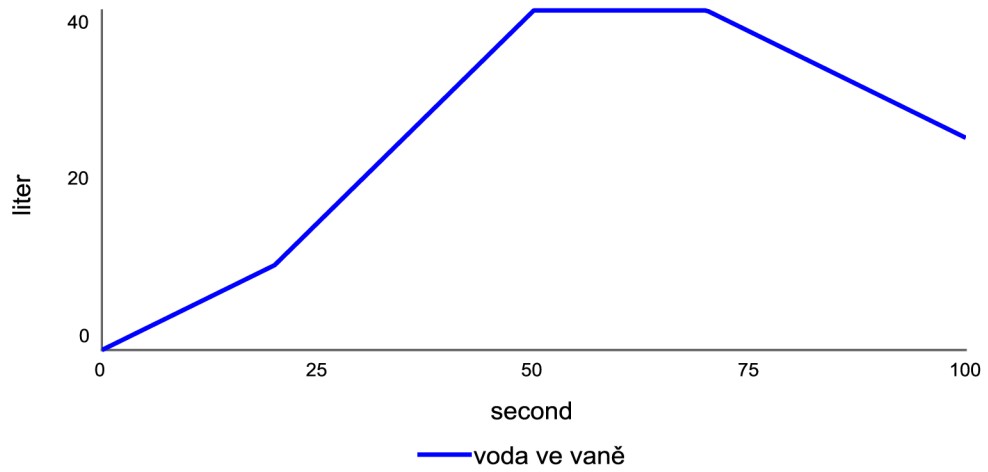
Klasickým příkladem je běžná vana (obr. 3). Vana samotná je reprezentována stavem, jehož hodnota udává množství vody ve vaně. Stavy jsou znázorňovány čtverci nebo obdélníky, zatímco složené šipky s kohouty představují toky. Symbol mraku představuje prvky, které jsou již za kauzální hranicí modelu. Všechny proměnné musí mít i svoji jednotku a v tomto případě se nabízí vodu ve vaně měřit v litrech a oba toky v litrech za sekundu. Z povahy věci vyplývá, že když přítok i odtok budou stejné, hladina vody ve vaně bude konstantní. Pokud přítok bude vyšší než odtok, hladina bude stoupat a naopak.

[44] Pozoruhodnou demonstrací univerzality a přenositelnosti těchto principů, která navíc vznikla zcela nezávisle na rozvoji systémové dynamiky, je stroj nesoucí jméno MONIAC. Je to vodou poháněný analogový hydraulický počítač, který byl zkonstruován v roce 1949 k simulaci národní ekonomiky Velké Británie. Veškeré procesy od míry zdanění až po investice jsou reprezentovány fyzickými nádržkami s vodou a spojovacím potrubím. Jedná se tak o unikátní a fungující materiální obdobu konceptuálních modelů systémové dynamiky (Bissell 2007).



Graf 1 – přítok a odtok vany

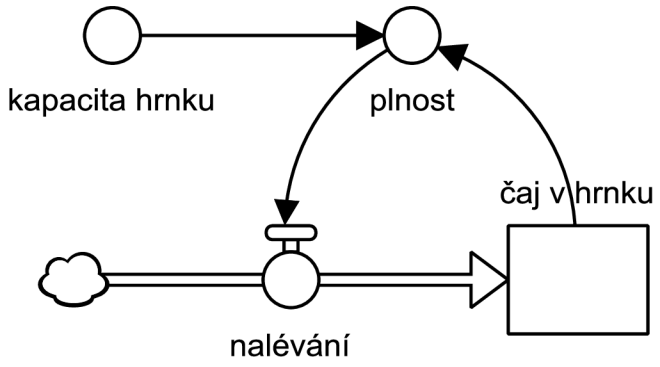
Na grafech je zachyceno, jak změny průtoků ovlivňují hladinu v této imaginární vaně. Přítok začíná na 0.5 litru za sekundu, ve dvacáté vteřině se zdvojnásobí a v sedmdesáté klesne zpět na 0.5 L/s. Odtok začíná na nule a po padesáti vteřinách se zvýší na 1 L/s, kde už zůstane až do konce simulace. Tempo změny hladiny tomu odpovídá.



Graf 2 – vývoj hladiny ve vaně

K demonstraci znázornění zpětné vazby je možné vanu vyměnit třeba za nalévání čaje do hrnku (obr. 4). Člověk nalévá čaj postupně, aby hrnek nepřelil. K tomu využívá zpětné vazby,

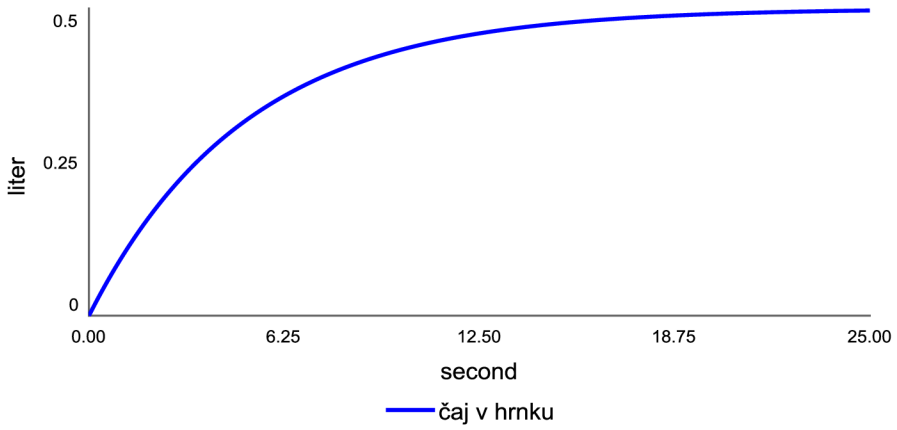
kterou mu poskytuje hladina čaje v hrnku. Čím více se hladina blíží k maximální kapacitě (resp. požadované hladině, pokud se liší), tím se zpomaluje nalévání.



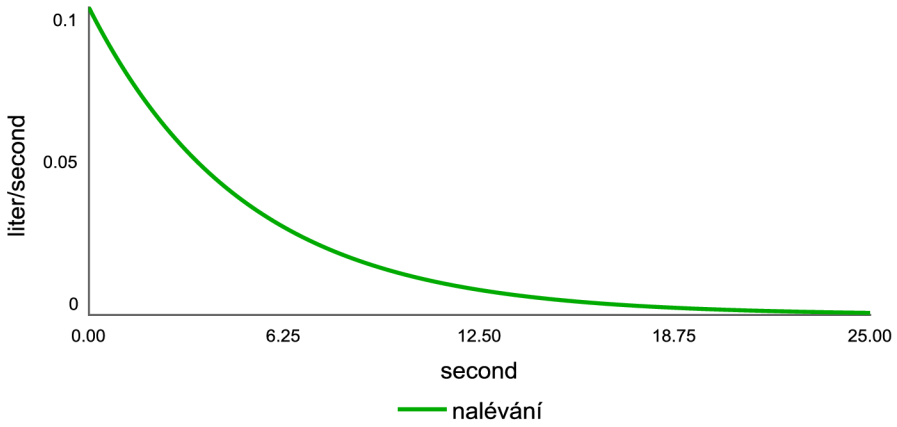
Obrázek 4 – jednoduchý diagram stavů a toků modelu hrnku s čajem

Zpětná vazba tak využívá měnící se informace o plnosti hrnku k tomu, aby regulovala rychlost nalévání. Plnost je v tomto modelu vyjádřena poměrem mezi kapacitou (konstanta o hodnotě 0.5 litru) a aktuálním stavem, tedy `plnost = čaj_v_hrnku/kapacita_hrnku`. Počáteční rychlost nalévání je 0.1 L/s, která ale klesá s rostoucí plností: `nalévání = 0.1*(1-plnost)`. Když objem již nalitého čaje roste a blíží se k maximální kapacitě hrnku, relativní plnost se přibližuje k 1 a tak je rychlost nalévání násobena činitelem, který se stejným tempem přibližuje k 0 a nalévání se tak zpomaluje (grafy 3 a 4). [45]

[45] Kromě tohoto zobrazení existuje i konvence ohledně pojmenovávání proměnných. Názvy konstant se píší celé kapitálkami, názvy stavů mají velké první písmeno každého slova a u zbytku jsou všechna písmena malá. Vzhledem k účelu této kapitoly je zde v zájmu jednoduchosti tato konvence záměrně opomenuta, nicméně předkládaný model protidžihádistického kybervigilantismu se jí samozřejmě drží (hlavní konvence viz Malczynski 2011).

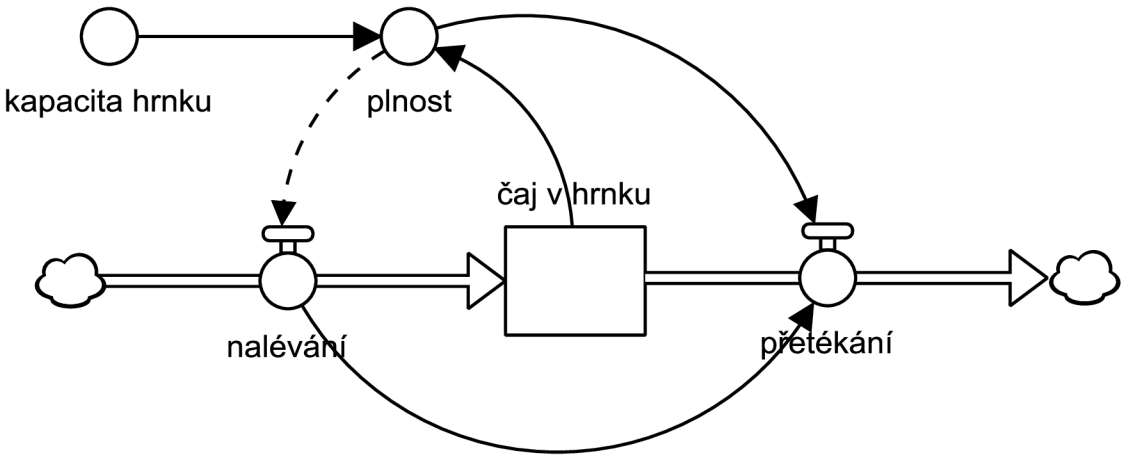


Graf 3 – vývoj hladiny čaje v hrnku



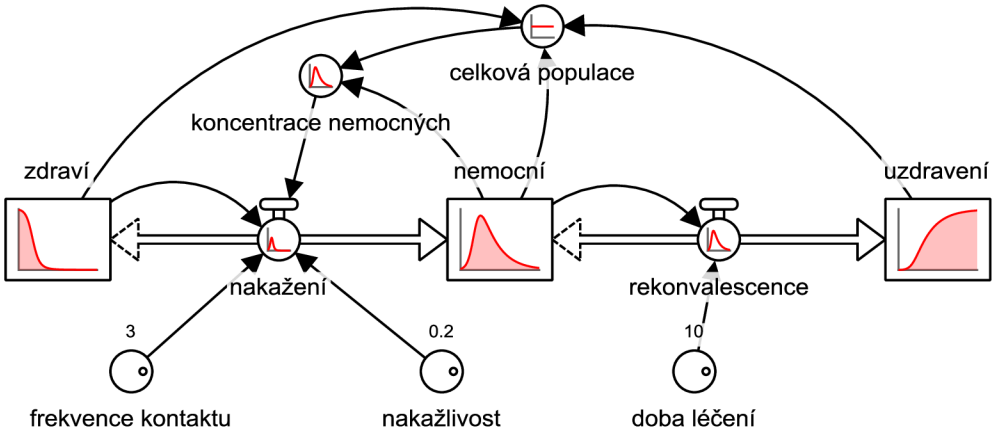
Graf 4 – přítok čaje do hrnku

Pokud dojde k selhání této zpětné vazby, která závisí na správné lidské reakci na vizuální podnět, bude rychlost nalévání konstantní bez ohledu na plnost hrnku a nakonec dojde k jeho přetečení přes okraj. I tuto eventualitu lze znázornit (obr. 5). V okamžiku, kdy hladina čaje překročí kapacitu hrnku, dojde k přetékání, které bude mít stejné tempo jako nalévání do již plného hrnku. Zároveň tím lze demonstrovat i využití logických a podmínkových funkcí v rámci systémové dynamiky: `přetékání = IF (plnost>1) THEN (nalévání) ELSE (0)`.



Obrázek 5 – rozšířený diagram stavů a toků modelu hrnku s čajem

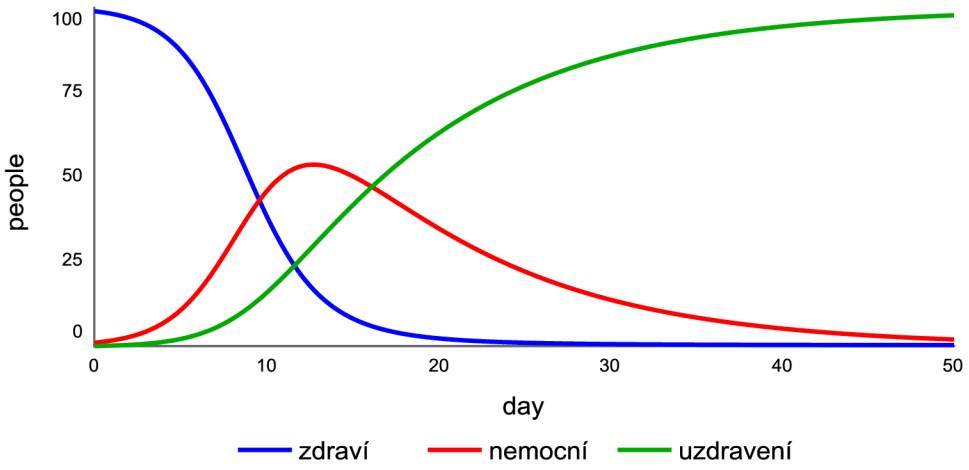
Častým chováním, které systémy vykazují, jsou takzvané S-křivky. Toto chování se objevuje tam, kde růst proměnné nejdříve zpětně urychluje její vlastní budoucí růst (tj. exponenciální růst, například úročení peněz v bance – čím více peněž je uloženo, tím větší jsou úroky a o to větší budou další úroky). Ale zároveň v systému existuje nějaké maximum, které tento růst omezuje, což je případ prakticky všech reálných a materiálních proměnných, neboť nic nemůže růst do nekonečna. Růst sledované proměnné se zpomaluje s tím, jak se přibližuje tomuto maximu, či nosné kapacitě systému (angl. *carrying capacity*). V grafu pak lze nalézt inflexní bod, kdy růst přestane akcelerovat a začne naopak zpomalovat (takže druhá derivace funkce je rovna nule).



Obrázek 6 – diagram stavů a toků modelu šíření nemoci (zde jsou proměnné zobrazeny i s pomocnými grafy jejich vývoje)

Toto chování lze demonstrovat na jednoduchém archetypálním SIR modelu (*Susceptible, Infected, Recovered*), který znázorňuje průběh nemoci v populaci (obr. 6). Rozlišuje tři stavy lidí – zdravé (tj. nakazitelné), nemocné (a zároveň nakažlivé) a již vyléčené (a tím i nenakazitelné). Zde zobrazená varianta začíná ve stavu, kdy se v modelu nachází celkem 100 lidí, z toho právě jeden nemocný a zbývajících 99 zdravých. K fyzickému kontaktu mezi lidmi, při kterém by mohlo dojít k přenosu nemoci, dochází 3x za den a nakažlivost je nastavena na 0.2 (takže každý pátý kontakt mezi zdravým a nemocným člověkem vyústí v přenos nemoci). Vyléčit se z této nemoci trvá 10 dní a uzdravený člověk získává imunitu, takže se již znovu nakazit nemůže.

Množství nově nakažených tím pádem závisí na tom, jak často dochází ke kontaktu mezi nemocnými a zdravými (tj. nakazitelnými).[46] V počátku jsou skoro všichni zdraví a tak může být nakažen prakticky každý, koho první nemocní potkají. Nemocných tak exponenciálně přibývá, neboť počet přenašečů stále roste. Jenže brzy (zde konkrétně během osmého dne) začne nakazitelných výrazně ubývat a ke konci jsou již téměř všichni buď nemocní nebo již nemoc prodělali. S-křivku lze proto vidět u vývoje počtu zdravých i uzdravených lidí, i když se od sebe liší směrem, sklonem i umístěním inflexního bodu (graf 5).

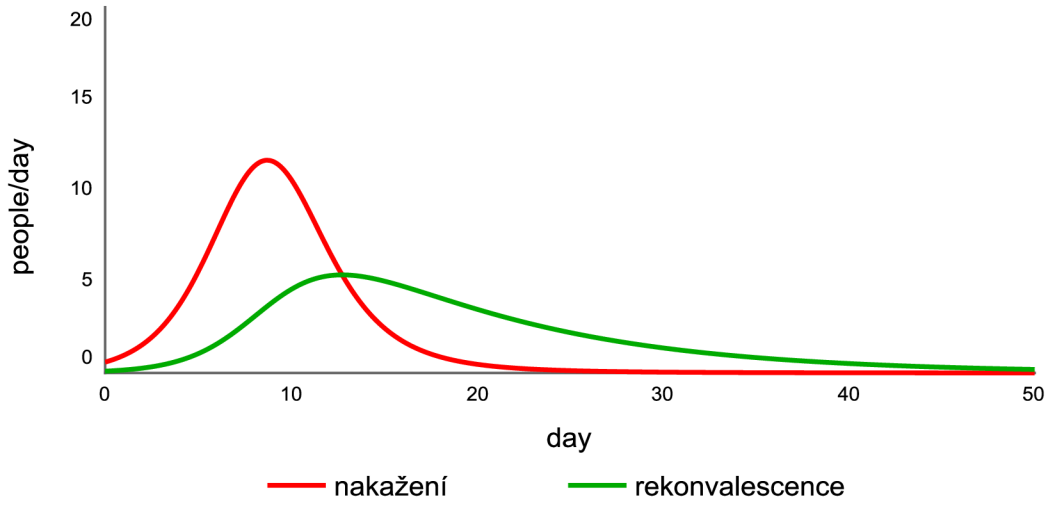


Graf 5 – graf vývoje počtů všech tří typů lidí v modelu šíření nemoci

[46] Výsledná rovnice pro výpočet nově nakažených i se substitucí:

```
nakažení = {koncentrace_nemocných}
            *zdraví*nakažlivost*frekvence_kontaktu
         = {nemocní/(zdraví+nemocní+uzdravení)}
            *zdraví*nakažlivost*frekvence_kontaktu
```

Inflexní body, tj. přesné momenty, kdy dojde ke změně a převáží jedna zpětná vazba nad druhou, lze lépe vidět na grafu toků (graf 6). Červená křivka má své maximum během osmého dne, tedy v ten moment přibývá nemocných a ubývá zdravých nejrychleji. Potom už se tok zpomaluje a tím se zpomaluje i úbytek zdravých lidí. Zelená křivka má své maximum v druhé polovině dvanáctého dne, kdy se uzdravení akumulují nejrychleji a dochází k inflexi u vývoje počtu uzdravených.

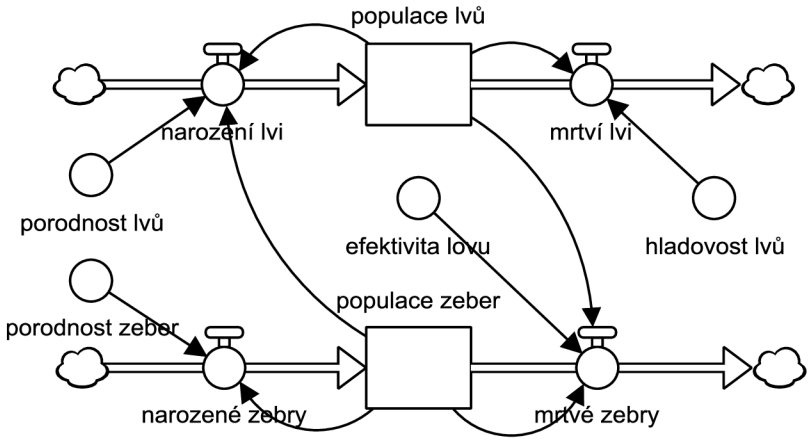


Graf 6 – graf vývoje velikosti toků v modelu šíření nemoci

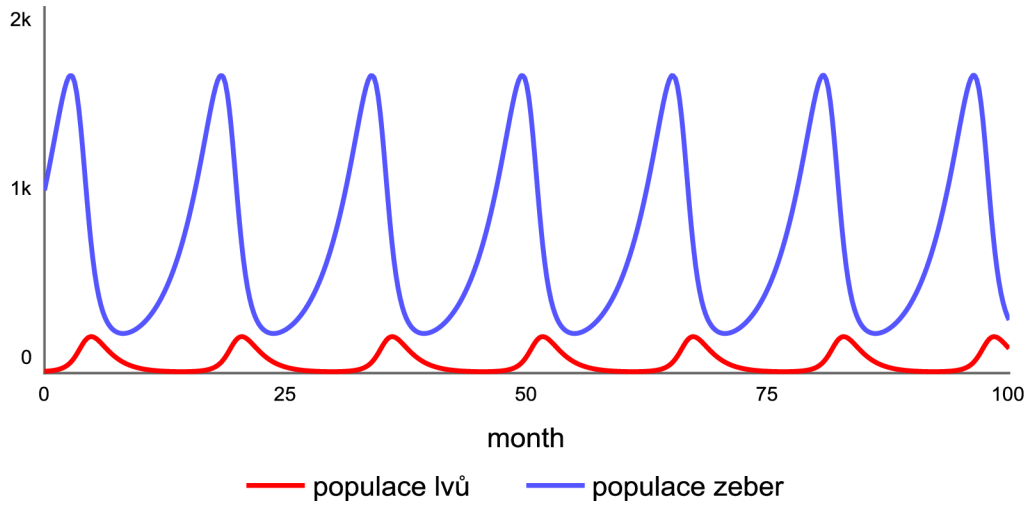
Kromě nemocí lze toto chování a S-křivky, kdy exponenciální růst narazí na nosnou kapacitu systému a je tím zbrzděn, pozorovat například i u vývoje lidské populace nebo tržním podílu nějakého produktu.

Pokud se v systému nachází zpoždění, takže zpětná vazba růst proměnné nezbrzdí včas, může dojít k oscilacím. Takový oscilující systém lze demonstrovat na dynamice predátorů a jejich kořisti, v tomto konkrétním případě lvů a zeber. Model (obr. 7) se skládá ze dvou stavů, jeden obsahuje populaci lvů a druhý populaci zeber. Rození nových zvířat a jejich smrt zachycují přítoky, respektive odtoky do obou stavů. Jednoduchá dynamika spočívá v tom, že lvi loví a žerou zebry. Rostoucí populace lvů způsobí vyšší úmrtnost mezi zebrami, neboť budou častěji loveny. Málo lvů má za důsledek málo ulovených zeber. Nicméně čím více se v oblasti pohybuje zeber,

tím lépe je mohou lvi lovit a sami se díky dostatku potravy množit. Naopak nedostatek zeber vede k hladovění a úhynu lvů.



Obrázek 7 – diagram stavů a toků modelu dynamiky predátorů a kořisti na příkladu lvů a zeber



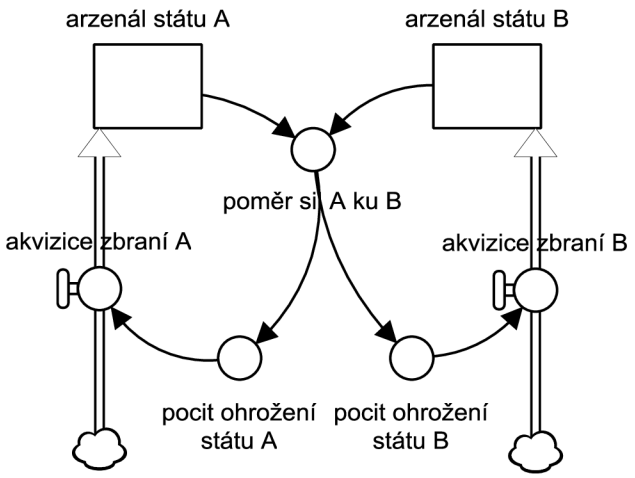
Graf 7 – graf cyklické dynamiky lvů a zeber (veškeré číselné hodnoty jsou zcela fiktivní a zvolené tak, aby byla v daném měřítku dobře viditelná souběžně oscilující velikost obou populací)

Na grafu je vidět výsledné chování takovéhoto zidealizovaného systému. Zebry nejdříve využijí relativní absence lvů a rychle se množí. Populace lvů ale také rychle stoupá, až dosáhne hladiny, kdy loví zebry rychleji, než se jejich počty stihají obnovovat. Následuje kolaps populace zeber a krátce na to i populace lvů, neboť najednou postrádají kořist. Díky tomu se zebry opět začínají množit a celý cyklus se opakuje. Ve skutečnosti nedochází k takto výrazným cyklům,

neboť se v ekosystému nachází mnoho dalších prvků, které toto chování ovlivňují (jiní predátoři, alternativní kořist pro lvy, výkyvy v množství dostupné trávy nebo vody atp.).

Pomocí diagramů stavů a toků lze zachytit a následně simulovat i situace podstatně bližší politickým vědám a bezpečnostním studiím. Klasickým případem je již zmíněná spirála zbrojení. Na obr. 8 lze nalézt jeden z mnoha způsobů, jak lze tento problém schematicky znázornit. Vojenské kapacity obou států jsou zde stavem a přítoky představují proces zbrojení. Rozhodující je poměr sil obou armád, od kterého plyne zpětná vazba skrze pocit ohrožení ke snaze tento poměr změnit ve prospěch té či oné strany. Když jedna strana zbrojí, mění tím poměr sil v neprospěch strany druhé, čímž u ní vyvolává její vlastní zbrojení. Výsledkem je neustále se posilující zpětná vazba a eskalující vzájemné zbrojení.

Pokud by se měl model více přiblížit realitě a obětovat tím něco ze své jednoduchosti, bylo by zapotřebí přidat prvky, které by znázorňovaly například omezenost zdrojů a ekonomickou náročnost zbrojení, politicko-strategické faktory, které by mohly spustit válečný konflikt, detaily procesu zbrojení, nebo větší množství aktérů (viz Drmola 2016 nebo Kreutzer 1985).



Obrázek 8 – diagram stavů a toků modelu závodů ve zbrojení mezi dvěma stranami

Na rozdíl od předchozích příkladů, u kterých byly všechny proměnné zcela exaktní a jednoznačně měřitelné, zde zobrazený model bezpečnostního dilematu je prvním příkladem komplexního sociálního systému. Zatímco proměnné zachycující počet lvů, kapacitu hrnku nebo

trvání nemoci mají jasný význam, hodnotu i jednotku, v sociálních systémech se vyskytují i proměnné bez těchto žádoucích kvalit.

V systémové dynamice často dochází k rozlišování takzvaných měkkých (*soft*) a tvrdých (*hard*) proměnných, respektive měkkých a tvrdých systémů. Toto dělení vychází právě z jejich exaktnosti a objektivní měřitelnosti. Tvrdé systémy mají blíže technickým oborům a přírodním vědám a jejich modelování lze obecně považovat za jednodušší, neboť hodnoty proměnných a vazby mezi nimi lze obvykle nějak jednoznačně změřit a vyjádřit. Měkké systémy jsou naopak ty, které obsahují i proměnné, jež takto měřitelné nejsou a podléhají subjektivní interpretaci. Prakticky všechny modely komplexních sociálních systémů (včetně tohoto konkrétního příkladu i celého modelu protidžihádistického vigilantismu v kyberprostoru) patří mezi měkké, neboť musí pracovat s proměnnými, jako je "strach", "důvěra" nebo "zručnost."[47]

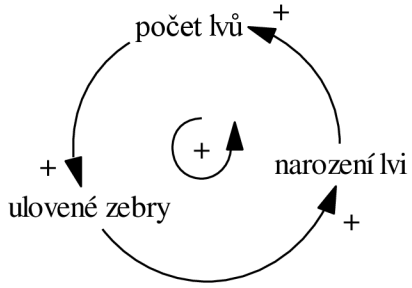
Snad by bylo možné nějak objektivně vyjádřit velikost zde zobrazených stavů (např. skrze množství bojové techniky, počet vojáků, velikost rozpočtu atp.), ale pro něco jako je „pocit ohrožení" neexistuje žádný měřitelný ekvivalent a rozhodně ani zavedená jednotka. Pokud se už někdo odhodlá pouštět se do modelování měkkých systémů, jsou v zásadě dva způsoby, jak se s tímto problémem vypořádat. Tím prvním je tyto proměnné do modelu vůbec nezahrnout a ignorovat je, neboť jsou nespolehlivé a dochází tím k zanesení subjektivity a zkreslení do modelu. Druhým způsobem, který je zcela dominantní, je tyto proměnné co nejlépe odhadnout a jejich hodnotu aproximovat.

Jejich ignorování je totiž mnohem horší chybou než nepřesný odhad. Pokud v modelu vůbec nebudou, značilo by to, že jejich vliv na chování systému je zanedbatelný, což obvykle není pravda. Navíc i u exaktních numerických dat může dojít ke zkreslení vlivem špatného sběru nebo interpretace. V každém případě je ale zapotřebí nakládat s nimi s obezřetností a hlavně otestovat chování modelu oproti historickým datům (tzv. *reference mode*). Při modelování komplexních sociálních systému se špatně uchopitelné měkké proměnné musí brát jako „nutné zlo" a spíše než je zavrhovat je nutné usilovat o co nejméně nepřesný odhad (Sterman 2000: 853-855).

---

[47] U zde popisované měřitelnosti se jedná spíše o její principiální vlastnost než o praktickou proveditelnost samotného úkonu měření. Například změřit hmotnost nějakého konkrétního kamene na povrchu jiné planety nebo na dně oceánu by nepochybně bylo extrémně obtížné až prakticky neproveditelné, ale přesto se jedná o „tvrdou" proměnnou, neboť v principu je zcela jednoznačně měřitelná a má jasnou jednotku. Tvrdost a měkkost tedy nerozlišuje, zda je výzkumník danou proměnnou schopen naměřit, ale zda je to vůbec teoreticky možné.

Vedle výše zobrazených příkladů diagramů stavů a toků je alternativním a jednodušším způsobem zobrazení modelů a systémů tzv. diagram kauzálních smyček (*causal loop diagram,* CLD).[48] Jedná se o abstrakci a redukci diagramu stavů a toků, která obsahuje přirozeně méně informací, ale je zpravidla přehlednější a jednodušší na pochopení. Prvky systému jsou nahrazeny jediným typem proměnných, které jsou spojeny kauzálními smyčkami. Některé proměnné jsou sloučeny do jiných nebo vynechány úplně, dle jejich důležitosti. Navíc ale přibývá označení polarity jednotlivých kauzálních smyček. Ty tak názorně zobrazují směr působení a zpětných vazeb. Polarita se nejčastěji značí znaménky + a - umístěnými podél šipky znázorňující příslušnou kauzální vazbu. + znamená, že růst první proměnné (odkud spoj vychází) zapříčiní růst druhé proměnné (kam spoj směřuje) a naopak pokles první způsobí i pokles druhé. Znaménko - značí, že růst první způsobí pokles druhé. Polarita spíše než nezávislý růst nebo pokles čehokoliv vyjadřuje souhlasnost nebo protichůdnost vývoje spojených proměnných.

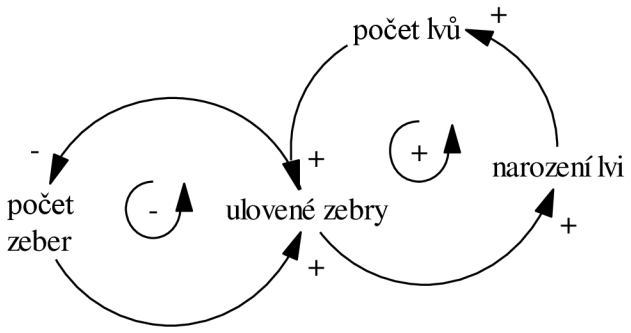


Obrázek 9 – redukovaný diagram kauzálních smyček vývoje populace lvů

Na obr. 9 je demonstrováno užití těchto symbolů. Všechny proměnné směřují stejným směrem. Za předpokladu, že je prozatím ignorována dynamika populace zeber, tak roste-li počet lvů, bude stoupat i jejich úlovek a tím pádem i schopnost odchovat další lvy. Roztáčí se posilující se (*reinforcing*) zpětná vazba, jejíž směr i polarita jsou zaznačeny v jejím středu.

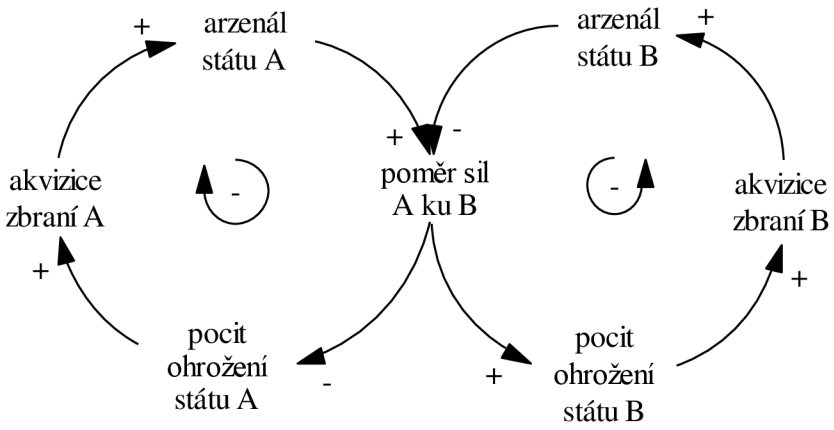
Diagram je možné „opravit“ přidáním populace zeber. Ty představují brzdu v systému, neboť jich není nekonečně mnoho. Eskalující lov zeber způsobí pokles jejich populace, což implikuje negativní vazbu a vyvažující (*balancing*) zpětnovazební smyčku.

[48] Na rozdíl od samotných modelů a všech diagramů stavů a toků (SFDs) bylo k tvorbě zobrazených diagramů kauzálních smyček (CLDs) použito i programu Vensim PLE x32 verze 7.0 od společnosti Ventana Systems, Inc., http://vensim.com/vensim-software/.



Obrázek 10 – diagram kauzálních smyček interakce lvů a zeber

Stejným zjednodušeným způsobem lze zpracovat předchozí model závodů ve zbrojení. Výsledkem jsou dvě spojené vyvažující se smyčky (obr. 11). I přestože jsou obě vyvažujícího typu, dávají svojí interakcí vzniknout eskalujícímu růstu tím, že se snaží vyvážit svoji hodnotu k neustále se posunujícímu cíli. Obě se snaží „dohnat“ rovnovážný stav, ale svým působením si jej navzájem neustále posunují dál a dál.



Obrázek 11 – diagram kauzálních smyček závodů ve zbrojení mezi dvěma stranami

Kromě větší přehlednosti a jednoduchosti lze tyto diagramy využít i jako předstupeň při vývoji úplného matematického modelu. Výzkumník si může vytvořit předběžný diagram kauzálních smyček jako první krok, aby si ujasnil roli hlavních prvků v systému, směr zpětných vazeb a také jako vodítko k nalezení nejvhodnější hranice modelu.

Na tyto diagramy lze také nahlížet jako na exaktnější verzi myšlenkových map a v některých případech mohou být i konečným produktem, obzvláště pokud konstrukce úplného matematického

modelu je z nějakého důvodu nereálná (například pokud je modelovaný systém příliš složitý nebo je alokován nedostatek času). Lze tak rozlišit kvalitativní a kvantitativní modelování systémů. Kvalitativní modely mohou výrazně přispět k lepšímu pochopení fungování systému, jsou přístupné většímu množství lidí, lze je aplikovat na širší spektrum systémů (obzvláště na ty měkké, viz Drmola – Bastl – Mareš 2015) a rozvíjejí tolik potřebné systémové myšlení. Oproti těm kvantitativním samozřejmě nejsou schopny simulací, jsou celkově méně přesné a mohou být příliš vágní až zavádějící, neboť je mnohem těžší je validovat vůči jejich reálným předlohám. Ideální je obě tyto metody znázornění modelů kombinovat (Wolstenholme 1998, Cavana – Mares 2008, Cioffi-Revilla 2014: 253-258).

Oba přístupy, kvalitativní i kvantitativní, napomáhají překonat neschopnost lidské mysli udržet a zároveň pracovat s větším množstvím konceptů, myšlenek či proměnných zároveň. Toto omezení lidem brání správně analyzovat chování složitých systémů, i pokud je dobře znají nebo dokonce jsou jejich součástí. Podle dnes již klasického psychologického výzkumu (Miller 1956) je člověk takto schopný pracovat jen s pěti až devíti prvky, zatímco komplexní modely se skládají z několikanásobně většího množství. Vizualizace těchto systémů a v ideálním případě i příprava simulací umožňuje soustředit se jen na zrovna zpracovávanou část modelu bez nutnosti pamatovat na strukturu a chování zbytku. Následně provádět simulace komplexních systémů bez pomoci počítačů je již zcela mimo možnosti lidí, neboť typicky obnášejí desítky proměnných a tisíce navzájem zřetězených kalkulací.

Kromě snadnějšího uchopení a porozumění problému je další výhodou možná redukce vlivu vlastní předpojatosti. Obzvláště u sociálních systémů bývá pro lidi (ať už jde o politika, novináře, akademika nebo důstojníka) obtížné oprostit se od vlastního, často i nevědomého, neobjektivního přesvědčení o tom, jak systém funguje nebo jak by měl fungovat (Yudkowsky 2008). Při čistě kvalitativní, neřkuli narativní, autorské práci může sehrát velkou roli subjektivní interpretace dat a mnohdy chybí interní mechanismus, jak toto zkreslení odfiltrovat a předkládané teorie a závěry validovat. Systémová dynamika a tvorba exaktních matematických simulací si jednak vynucuje vnitřní konzistenci modelů (např. skrze integritu jednotek jednotlivých proměnných) a navíc umožňuje porovnání simulovaného chování vybudovaného modelu s pozorovaným chováním jeho reálné předlohy.

4.2 Chaos a mocninné zákony

Jednou z největších překážek stojící v cestě modelům a simulacím terorismu a jeho interakci s čímkoliv je extrémně obtížná předvídatelnost jednotlivých útoků. V prvé řadě už jen výběr místa a času útoku není v našich silách účinně předpovědět. Není sice těžké vyhodnotit, jaké typy cílů jsou atraktivní a jaké bývají často napadány (obvykle tzv. měkké cíle, s velkou koncentrací civilistů a s vysokou symbolickou hodnotou), ale vzhledem k obrovskému množství těchto potenciálních cílů, které se v našich městech nacházejí, a relativně nízkému počtu teroristických útoků, ke kterým přeci jen dochází, je prakticky nemožné vybrat ten, která napaden opravdu bude. To samé platí o volbě dne a hodiny útoku.

Tento problém se dále stupňuje i během samotného útoku. Pokud bychom chtěli předpovědět počet obětí konkrétního teroristického útoku, ani znalost jeho času a místa nám příliš nepomůže. Kolik se na něm bude podílet útočníků? Jaké použijí zbraně a jak dobře s nimi umějí zacházet? Co když některé z nich selžou (typicky podomácku vyráběné improvizované výbušniny)? Kolik bude na místě lidí a nebude někdo z nich také ozbrojen? Je poblíž zrovna nějaká hlídka policie? Jak rychle ji někdo zavolá a jak bude reagovat? Počet navzájem nezávislých proměnných velice prudce narůstá a jejich výsledné interakce se stávají nepředvídatelnými (viz Bakker 2012, Telesca - Lovallo 2006, Fellman - Wright 2004).

Takovýto systém lze označit jako chaotický, tedy extrémně citlivý na počáteční parametry. I zcela nepatrná změna má obrovský dopad na následné chování systému. Posunutí útoku o minutu může způsobit, že bude předčasně odhalen a zmařen. Posunutí vodiče o centimetr může způsobit předčasnou detonaci vyráběného výbušného systému. Pokud tuto parametrickou citlivost spojíme s faktem, že tyto parametry dopředu ani neznáme a můžeme je jen velmi zhruba odhadovat na základě předchozích zkušeností, dostáváme se k systému, jehož chování nedokážeme předvídat.[49]

Jednou z možností, jak se při systémovém modelování lze s tímto problémem vypořádat, je užít průměrných hodnot. Není těžké spočítat průměrný interval mezi teroristickými útoky ani

[49] Toto lze dobře ilustrovat na proběhnuvších útocích, které měly docela podobné počáteční parametry ale diametrálně odlišné výsledky. Například útoky za pomocí improvizovaných výbušnin v tlakových hrncích (tzv. papiňácích) patří k těm nejpopulárnějším již mnoho let, vždy cílí na hustě zalidněná místa a přesto se počty takto způsobených obětí liší o několik řádů. Zatímco třeba v Bostonu (2013) nebo v Bombaji (2006) připadalo na každou takovou detonovanou bombu více než sto mrtvých a zraněných, jindy (např. Stockholm, New York) to bylo méně než pět nebo dokonce k detonaci vůbec nedošlo. Stejně široké rozpětí můžeme nalézt i v případě ostatních typů teroristických útoků – ať už najetím vozidlem nebo střelbou ze zbraně (viz START 2017, RAND 2017).

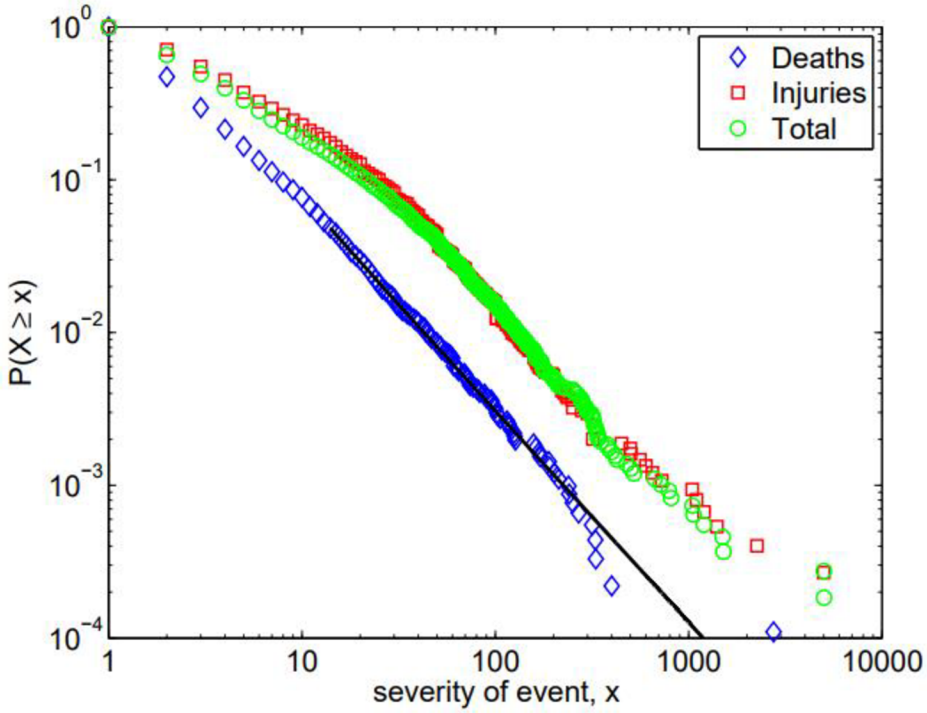
průměrné počty obětí, ke kterým při nich dochází. Pokud by ale teroristické útoky, které vlastně celému systému udávají tempo, byly takto zprůměrovány a "vyhlazeny", ztratil by se dynamický charakter celého systému, který ve skutečnosti vzniká reakcemi jeho jednotlivých prvků na děje uvnitř něj, a nebyly by adekvátně reprezentovány prudké výkyvy, kterými systém prochází po významných útocích.

Alternativním způsobem, jak k těmto jevům přistupovat, je simulovat jejich historicky vypozorované pravděpodobnostní rozdělení na agregované úrovni. Přestože nedokážeme mnoho říci k žádnému konkrétnímu teroristickému útoku, je možné matematicky vyjádřit, jaké procento z celé množiny útoků vyústí v ten či onen počet obětí nebo kolik se na něm bude podílet teroristů. Marná snaha simulovat jednotlivé teroristické útoky v celé jejich kauzální komplexitě je tak nahrazena pravděpodobnostním modelem, který výsledky (resp. teroristické útoky) generuje dynamicky.

Základem pro tento model je mocninný zákon (angl. *power law*), který charakterizuje distribuci závažnosti teroristických útoků z hlediska počtu jejich obětí. Takovéto mocninné zákony lze ale identifikovat v mnoha fyzikálních, biologických i sociálních jevech a metodologicky patří mezi jedny z nástrojů analýzy komplexity v rámci komputativních sociálních věd. Známou formou těchto zákonů je tzv. Paretovo pravidlo, někdy vyjadřované jako "80/20" - například, že 20% lidí vlastní 80% pozemků, nebo že 20% zákazníků generuje 80% tržeb. Jako příklady této distribuce lze uvést velikost měst, velikost kráterů, frekvenci jmen, prodejnost knih, velikost zvířat a další. Pozoruhodné je, že z doposud neobjasněných důvodů se tento vztah nejčastěji vyskytuje u proměnných vyjadřujících velikost nějakého jevu a téměř nikdy jeho dobu trvání (Newman 2004, Cioffi-Revilla 2014: 152-169). Milníkem v této oblasti byl Richardsonův (1960) objev, že tímto zákonem se řídí i mezistátní války. Tyto principy byly později rozšířeny i na povstalectví, guerillové války a terorismus (viz Bohorquez - Gourley - Dixon - Spagat - Johnson 2009, Johnson – Carran et al. 2011).

Klíčovou charakteristikou všech těchto mocninných distribucí je jejich extrémně dlouhý chvost funkce. Obvykle se většina případů z dané množiny nachází u minimálních hodnot. Přitom ale existuje malé množství případů, které leží v extrémních hodnotách. V případě terorismu to vypadá tak, že velká většina útoků má jen minimální množství obětí, typický méně než deset. Případy s více než sto oběťmi jsou poměrně neobvyklé. A zároveň existují vzácné extrémy, jako bylo 11. září 2001, které leží daleko na chvostu funkce vyjadřující tuto distribuci. Tyto obrovské

útoky jsou sice velmi nepravděpodobné, ale neexistuje pro ně žádné maximum, které by nemohly překročit (Clauset - Woodard 2013).[50]

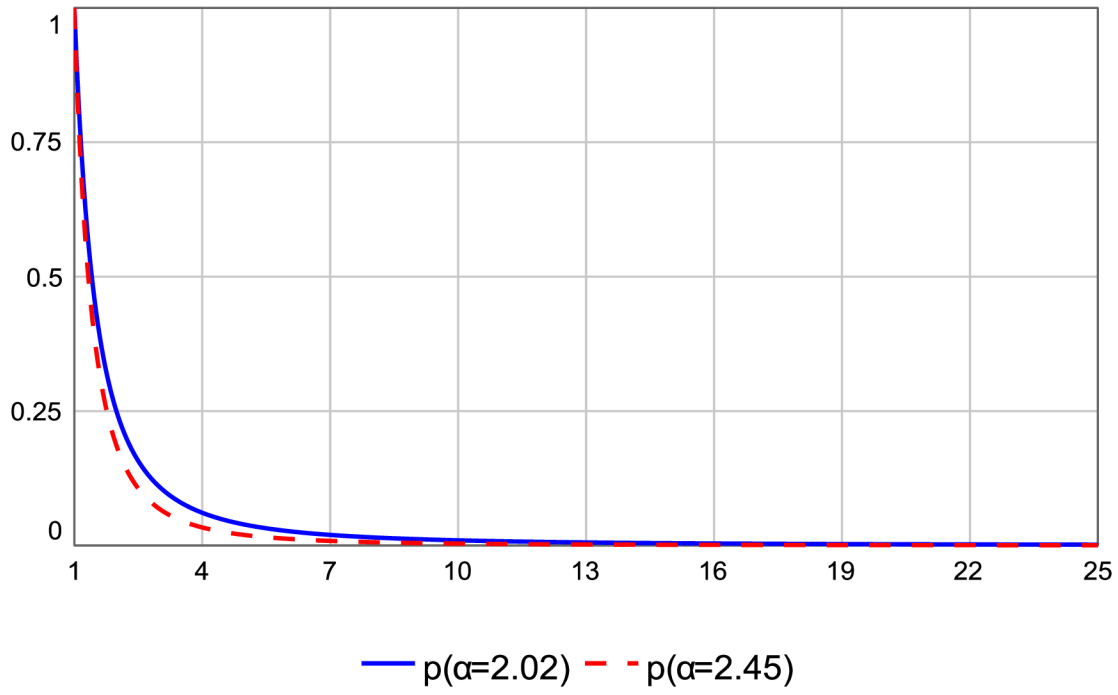


Graf 8 – demonstrace průběhu mocninného zákona a vztahu mezi frekvencí teroristických útoků a počtem jejich obětí (na tomto grafu je znázorněn přímkou, neboť používá logaritmické stupnice namísto lineární), zdroj: Clauset - Young - Gleditsch 2007

Tuto pravděpodobnostní funkci lze vyjádřit jako $p(x) \propto x^{-\alpha}$, kde *x* značí počet obětí a α je exponent, který udává sklon takto generované křivky (*scaling exponent*). Podrobnější analýza teroristických útoků odhalila i mírné rozdíly ve tvaru těchto pravděpodobnostních funkcí pro jednotlivé regiony a typy zbraní. Pro účely této práce je použit exponent 2.02 (Clauset - Young - Gleditsch 2007), který platí pro země OECD. Pro ilustraci lze uvést, že například pro konflikt v Afghánistánu byl nalezen exponent 2.45 (Johnson - Spagat et al. 2006), který generuje prudčeji

[50] Tento typ pravděpodobnostní distribuce tak kontrastuje s lépe známým Gaussovým (též zvaným "normálním") rozdělením pravděpodobnosti, které je naopak charakteristické nejfrekventovanějším středem a symetrickými omezenými chvosty po jeho stranách. Klasickým příkladem je distribuce výšky v lidské populaci. Většina lidí má "normální" výšku kolem 160-180 centimetrů (v závislosti na pohlaví) a relativní výskyt klesá s odchylkou od tohoto středu na obě strany. Dospělých lidí větších než 250 nebo menších než 100 centimetrů je opravdu velmi málo. Pokud by se výška naopak řídila mocninným zákonem, měla by valná většina populace třeba metr a půl a zároveň by se vyskytovali lidé přes tři metry (viz Bibighaus 2015: 39-43 a srovnávací ilustrace v příloze).

klesající křivku, a tudíž větší převahu malých útoků nad velkými. Na grafu 9 je pro ilustraci zobrazen průběh obou funkcí. Přestože vypadají velmi podobně, pro $x = 20$ je $p(\alpha = 2.02)$ asi 3.6x vyšší, než $p(\alpha = 2.45)$.[51]



Graf 9 – ilustrativní srovnání průběhu funkce p(x) = x^(-α) pro dvě různé hodnoty α

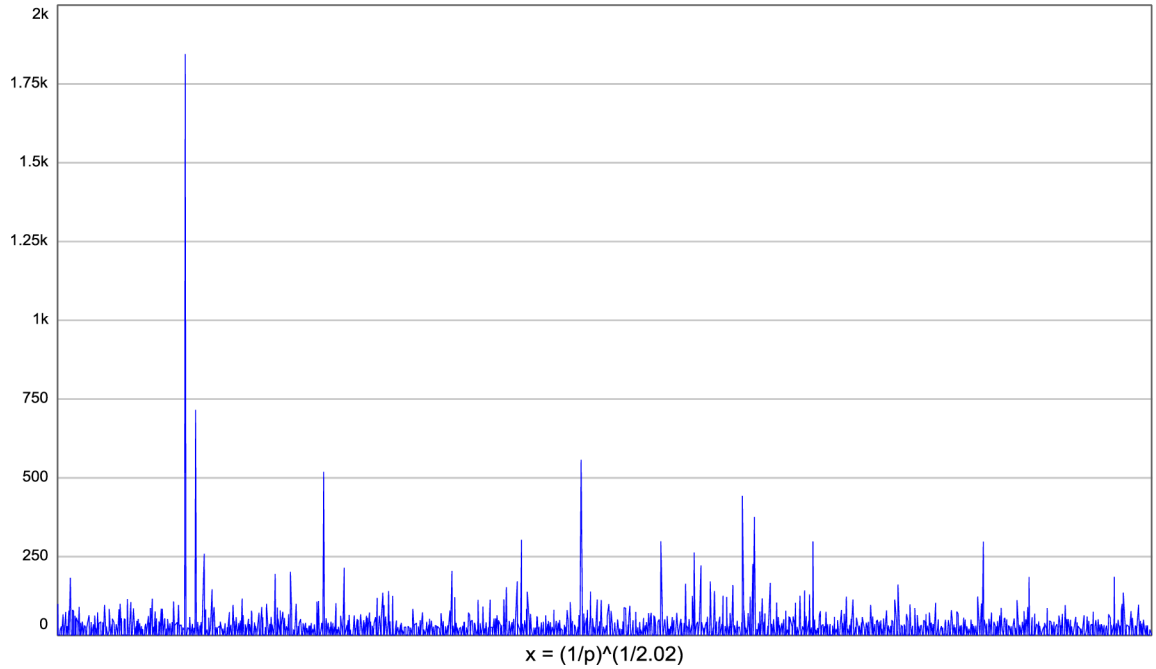
Je také důležité upozornit, že tyto funkce nevypovídají vůbec nic o tom, jak často k teroristickým útokům jako takovým obecně dochází. Vyjadřují pouze pravděpodobnostní rozdělení množství obětí u útoků, ke kterým došlo. Správná interpretace tedy je, že pokud už proběhne teroristický útok, je pravděpodobnost, že při něm dojde asi ke dvaceti obětem, zhruba třiapůlkrát vyšší v zemích OECD než v Afghánistánu. Nikoliv, že by v nich k útokům o dvaceti obětech docházelo třiapůlkrát častěji (Clauset - Wiegel 2010, Clauset - Young - Gleditsch 2007, Johnson - Spagat et al. 2006).

Tato funkce tedy vyjadřuje pravděpodobnost p, že útok způsobí daný počet obětí x. Pro využití v systémovém modelu je však tuto funkci zapotřebí převrátit, neboť počet obětí je právě ta

[51] $p(x = 20, \alpha = 2.02) = x^{-\alpha} = 20^{(-2.02)} \approx 0.0023546$
$p(x = 20, \alpha = 2.45) = x^{-\alpha} = 20^{(-2.45)} \approx 0.0006493$
$\frac{0.0023546}{0.0006493} \approx 3.6261260$

hodnota, již je potřeba vygenerovat, aby tím mohla být reprezentována chaotičnost teroristických útoků. Jednoduchou matematickou úpravou tak vzniká výraz $x \propto \sqrt[\alpha]{1/p}$. Při známém exponentu $\alpha = 2.02$ je s tímto výrazem možné generovat příslušné počty obětí x je-li dodána hodnota p. V tomto opačném směru je p náhodným (nebo spíše pseudonáhodným) [52] číslem uvnitř modelovacího softwaru. Má-li být tedy spočítán výsledný počet obětí simulovaného útoku, je do této převrácené funkce dosazeno náhodné číslo v rozmezí 0 až 1, pro které je tak nalezen odpovídající výsledek. Graf 10 ilustruje korespondující rozložení výsledků tohoto procesu a je na něm zachycen přesně 1 milion cyklů. Nicméně i přes zdánlivě vysoké generované hodnoty je průměr $\bar{x} = 1.98$, což dobře poukazuje na fungování mocninného zákona a na celkovou převahu relativně malých hodnot i za přítomnosti extrémů z chvostu funkce.

[52] V úzkém slova smyslu se nejedná o číslo opravdu náhodné nýbrž pseudonáhodné. Pravou náhodnost je překvapivě obtížné nalézt. Vlastně všechny jevy, které ve svém běžném životě považujeme za náhodné, jsou ve skutečnosti chaotické – tedy prakticky nepředvídatelné, protože jsou extrémně citlivé na výchozí podmínky, které nedokážeme dostatečně přesně pozorovat nebo ovlivnit. To ale zároveň znamená, že jsou deterministické, tudíž teoreticky předvídatelné a v predikcích nám brání jen vlastní nedokonalé znalosti těchto systémů a příliš velké množství proměnných, jež nedokážeme dosti přesně a rychle měřit (viz předpovědi počasí). Jako příklady těchto chaotických systémů, jejichž chování se může zdát náhodné, lze uvést hod kostkou, hod mincí, kulečníkový rozstřel nebo losování sportky. Člověk nedokáže kontrolovat všechny proměnné, které ovlivňují hod kostkou, ale dostatečně precizní robot nad fixní podložkou by nepochybně neměl problém hodit vždy stejné číslo. Podobně problematické je i generování náhodných čísel uvnitř počítačů, což je případ i tohoto modelu. I ty vznikají deterministicky. Vykazují ovšem dostatečně vysokou entropii a pro téměř libovolné praktické použití (s možnou výjimkou kryptografie) je lze bez obav považovat za náhodné. Pro tyto generátory čísel se užívá pojem pseudonáhodné. Momentálně jsou za jediný známý zdroj pravé náhody považovány jevy z domény kvantové mechaniky (Eagle 2016, Barker - Kelsey 2015).



Graf 10 – graf výsledných hodnot funkce $= \sqrt[2.02]{1/p}$ *, kde p je náhodně generované číslo v intervalu [0, 1], po milionu opakování*

Uvnitř modelu tím tedy vznikají dynamicky generované počty obětí simulovaných teroristických útoků, které svojí pravděpodobnostní distribucí zcela odpovídají počtům obětí při reálných (chaotických) útocích. V modelu tak s odpovídající pravděpodobností může docházet k útokům běžně malým i k těm extrémně vzácným, které zastíní i ty z 11. září 2001. Jedná se tedy o model stochastický a každá simulace tohoto modelu je zcela jedinečná a neopakovatelná, protože závisí na unikátní sekvenci náhodně generovaných čísel.

4.3 Parametry, kompromisy a vymezení modelu

V důsledku této integrace mocninných zákonů do modelu dochází k jistému vybočení ze standardů systémové dynamiky, neboť valná většina modelů vznikající v rámci této metodologie je zcela deterministická a žádné náhodně generované prvky neobsahuje. Takže zatímco u většiny modelů dynamických systémů se lze spokojit s výsledkem jediné simulace a ten považovat za definitivní (neboť každá další by proběhla zcela identicky), v tomto modelu je každý výsledek jedinečný. Není proto možné vyvozovat jakékoliv závěry z libovolné jedné simulace a pro jakoukoliv smysluplnou analýzu výsledků je nutné pracovat s velkými vzorky opakovaných běhů. V této práci je velikost vzorku stanovena na 10000 pro každé jednotlivé nastavení modelu a každý scénář.[53] Tato hodnota je dostatečná pro zaručení spolehlivosti a konzistentnosti výsledků.[54]

Omezení spíše technického charakteru vyplývají z rozhodnutí simulovat teroristické útoky jako jednorázové události (*discrete events*), což opět není systémové dynamice zcela vlastní. V tomto modelu je jako základní časová jednotka zvolen týden jako vhodný kompromis mezi detailností a agregovaností. Za normálních okolností by pro účel výpočtu vývoje jednotlivých toků a stavů byla i tato časová jednotka rozdělena na menší kroky. Tento interval se označuje jako dt (*delta time*) a udává, na jak malé kroky je základní časová jednotka rozdělena. Někdy se uvádí ve formě zlomku, například dt = 1/4 nebo 1/32.[55] Čím menší dt je nastaveno, tím přesnější je model, neboť všechny hodnoty jsou rekalkulovány častěji. Zároveň se tím ale zvyšuje náročnost a model se tak zpomaluje (více k *delta time* viz Sterman 2000: 232-241).

Tohoto však bohužel nelze užít v případě jednorázových dějů, které jsou v modelu implementovány skrze pseudonáhodné mocninné funkce, a proto je zde užito „pouze“ dt = 1. To

---

[53] Tato hodnota ovšem platí pouze pro zde prezentované finální výsledky. Během vývoje a ladění modelu bylo z časových důvodů používáno mnohem menších vzorků (většinou 500 simulací), neboť každá změna struktury či parametrů musela být otestována. Důvodem byl vysoký počet pracovních verzí modelu (několik set) a jeho výpočetní náročnost. Výpočet celé jedné série deseti tisíc simulací v horizontu dvaceti let (tj. přes 10 milionů cyklů modelu) trvá na běžném počítači kolem dvaceti minut.

[54] K vyprodukování a exportu dat z takto velkého počtu simulací je využito funkce “analýzy citlivosti” (angl. *sensitivity analysis*), která původně k takovýmto účelům sice neslouží, ale po nastavení je toho schopna. V modelu se nachází pomocná a k ničemu nepřipojená (a tudíž pro chování systému zcela irelevantní) proměnná nazvaná *S-VAR*, na které je spuštěna analýza citlivosti pro hodnoty 0 až 1 s požadovaným počtem inkrementálních mezikroků (například 10000). Takto vygenerovaný výstup je pak k dalšímu zpracování exportován do MS Excel.

[55] Aby se předešlo zkreslení ze zaokrouhlení při převodu do binární číselné soustavy, ve které počítač kalkulace provede, měl by při použití zápisu dt pomocí zlomku jmenovatel být kladnou celočíselnou mocninou 2. Při standardním zápisu pomocí desetinného rozvoje jsou ekvivalentem záporné mocniny 2. Aneb například: dt = 1/16 = $1/2^4 = 2^{-4}$ = 0.0625

je částečně kompenzováno použitím přesnější integrační metody a namísto standardní Eulerovy integrace je použito složitějšího algoritmu Runge-Kutta čtvrtého řádu (RK4), který využívá přesnějších aproximací změn stavů a toků v časovém intervalu dt (Sterman 2000: 907-911).

Jedním z hlavních zjednodušení modelu je, že nerozlišuje mezi zraněnými a mrtvými oběťmi teroristických útoků a kombinuje je do jediné proměnné sdružující všechny oběti (*casualties*). Rozlišování obou typů obětí by značně zvýšilo komplexitu modelu, aniž by to přineslo nějaké důležité poznatky, neboť systém na ně reaguje podobně a hlavně se jejich distribuce řídí mocninným zákonem o stejném exponentu (viz Clauset - Young - Gleditsch 2007). Celkový počet obětí je jednoduše vypočítán jako suma počtu zabitých a jedné desetiny zraněných, což by mělo přibližně reflektovat relativní sílu reakce, které tyto typy obětí v systému dále vyvolávají.

Model je ohraničen v čase i prostoru (viz kapitola Cíle). Desetiletý horizont 2007-2016 vychází jednak z dostupnosti dat a také z pozorovaného chování systému, které bylo prvních osm let poměrně homogenní a klidné. Pokud by byl zkoumaný časový úsek třeba o dalších deset let delší, obsahoval by jednak příliš mnoho výkyvů a navíc zcela by postrádalo smysl zaměřovat se na roli kyberprostoru, hacktivismu a vigilantismu, neboť tyto faktory začaly hrát významnou roli až v poslední dekádě.

Omezení na „Západ“ plyne z politické, strategické, mediální i kulturní blízkosti. Přestože teroristické útoky jsou častější mimo tuto oblast, nevyvolávají tak silnou reakci ve zbytku systému a ani nejsou tak silně provázané s kyberprostorem. Z etického hlediska na to lze pohlížet všelijak, ale model by měl reflektovat skutečné fungování systému, a pokud je cílem modelovat i interakce v kyberprostoru, bylo by zahrnutí naprosto všech džihádistických teroristických útoků (např. těch na Blízkém východě) zkreslujícím faktorem. Je to právě Západ, kde hraje kyberprostor významnou roli při radikalizaci, odkud působí většina hacktivistů, a kde útoky vyvolávají nejsilnější odezvu. Západ je pro účely této práce vymezen jako: státy Evropského jednotného trhu (EU+EFTA), Spojené státy americké, Kanada, Austrálie a Nový Zéland (celkem 885 milionů lidí). Navíc právě v těchto zemích jsou teroristické útoky označovány jako forma boje proti tzv. vzdálenému nepříteli, případně jako odplata za jejich intervence na Blízkém východě. Západ, i když jeho přesné ohraničení se může mezi autory mírně lišit, představuje v kontextu džihádismu specifickou arénu (viz Hegghammer 2016, Vidio - Marone - Entemann 2017, Nesser - Stenersen – Oftedal 2016).

Poslední poznámka se vztahuje k jazyku. Přestože celá práce je v českém jazyce, model samotný (tj. názvy proměnných a funkcí) používá anglickou terminologii. Primárním důvodem je

srozumitelnost a kompatibilita tohoto modelu v rámci širší komunity systémové dynamiky, která je celosvětová[56] a pracuje takřka výhradně v anglickém jazyce (česká komunita je obzvláště malá). Podobně i všechny modelovací programy a názvy funkcí i systémových prvků užívají jednotnou terminologii v anglickém jazyce. Překlad celého modelu do češtiny by tak byl spíše kontraproduktivním počinem, obzvláště když je celý česky popsán a vysvětlen.

[56] Zastřešující organizací je *System Dynamics Society*: http://www.systemdynamics.org/.

5 Související výzkum

Tato práce v žádném případě nepředstavuje první snahu o aplikování systémové dynamiky na výzkum terorismu. Naopak se opírá a čerpá z předešlého výzkumu. Co se týká základní struktury a způsobu zachycení terorismu a radikalizace, největší inspirací byly modely od Nazli Choucri a jejího týmu (2007) a dvojice Pruyt a Kwakkel (2014). Přestože oba modely (respektive celkem tři, protože Pruyt a Kwakkel prezentují svoje modely dva) mají mírně odlišné zaměření, ve svém jádru sdílejí archetypální SIR strukturu (viz kapitola 4.1.4), kterou zde v modifikované podobě používá i model protidžihádistického vigilantismu v kyberprostoru. Choucri a její tým modelovali státní stabilitu a šíření subverzivní ideologie, která populaci transformuje postupně v disidenty a nakonec ve vzbouřence, kteří stabilitu podrývají. Pruyt a Kwakkel se zabývají explicitně terorismem a k němu směřující radikalizací jakožto procesem, který je důsledkem vnímaných a neadresovaných křivd. Nicméně v obou případech je proces radikalizace (případně „disidentizace“) modelován způsobem, který lze přirovnat k šíření nemoci skrze populaci, přičemž existující vzbouřenci (*insurgents*) a teroristé fungují jako „přenašeči“ a „nakažlivost“ se odvíjí od jejich schopnosti šířit svoji ideologii napříč společností.

Vedle radikalizace existují i extenzivní modely zaměřené přímo na vzbouřenectví či guerillovou válku. Tyto se ale spíše zabývají dynamikou kontroly území a populace a soupeřením s místní státní mocí. Díky své aktuálnosti zde za zmínku určitě stojí Clancy (2016a), který modeluje a zkoumá Islámský stát optikou protostátu (*emergent state actor*), včetně jeho nečekaně rychlého rozmachu, který koreloval s nárůstem vlivu džihádismu a frekvence teroristických útoků na Západě. Dalším počinem z této oblasti, ze kterého i Clancy částečně vychází, je dřívější model Andersona (2011), který je vybudován na základě dat z průběhu Britsko-irské války za nezávislost v letech 1919-1921 a konceptů z amerického vojenského protipovstaleckého polního manuálu (*US. Army and Marine Counterinsurgency Manual*, FM 3-24). Jako další příklady lze uvést analýzu fungování a struktury teroristických organizací (Schoenenberger - Schenker-Wicki - Beck 2012) nebo model dopadu různých protiteroristických politik (Leweling – Sieber 2007).

O poznání skoupější je pole aplikací této metody na otázky kybernetické bezpečnosti. Na rozdíl od modelu terorismu zde ani není možné identifikovat nějaký sdílený a zavedený archetyp, na který by bylo možné navázat. Důvodem je především relativní novost této zájmové oblasti oproti terorismu a také ještě horší dostupnost dat. I přesto existují práce, které konflikty

v kyberprostoru modelují – například modely mezinárodního konfliktu v kyberprostoru (Armenia – Cardazzone – Carlini 2014, Polatin-Reuben – Craig – Spyridopoulos – Tryfonas 2013), nebo fungováním kybernetických hrozeb a aktérů uvnitř chráněného systému (Greitzer et al. 2008, Armenia – Tsaples 2016, Band et al. 2006, Rich – Martinez-Moyano – Conrad et al. 2005). Nicméně vzhledem k tomu, že se zabývají odlišnými aspekty kyberprostoru a jinými formami útoků, ke kterým v něm dochází, tak zde předkládaný model na ně moc nemá jak navázat.

I mezi výzkumnými aplikacemi mocninných zákonů převažuje tématika terorismu nad kybernetickou bezpečností. Většina klíčových prací (tj. především Clauset - Young - Gleditsch 2007 a Johnson – Spagat et al. 2006) byla již zmíněna v předchozí kapitole o metodologii, neboť jsou kromě koncepční inspirace zdrojem i konkrétní hodnoty exponentu pravděpodobnostní funkce použité v modelu. Vedle těchto teoretických prací je tou nejvýznamnější aplikací nejspíše odhalení vzájemné adaptivní eskalace aktivit teroristických a vzbouřeneckých skupin v konfliktních zónách ve vztahu ke zde dislokovaným ozbrojeným silám. Autoři (Johnson – Carran et al. 2011) odhalili dynamiku srovnatelnou s tzv. „efektem červené královny“ známým z evoluční biologie (název má původ v *Alence v říši divů* od L. Carrolla), kdy se obě strany konfliktu musí neustále vyvíjet, přizpůsobovat a inovovat, jen aby udržely *status quo* a krok s konkurentem. Ve výsledku se tak žádná strana vlastně nezlepšuje v tom, co dělá (ať už jde o biologický druh nebo teroristickou skupinu), i přestože na adaptaci vynakládá velké úsilí a prostředky, protože neustále jen reaguje na tlaky z okolí.

V kontextu kybernetické bezpečnosti a konfliktů v kyberprostoru lze najít několik prací, které na kybernetické útoky aplikují stejné metody, jaké byly výše uplatněny v případě teroristických útoků. Jedná se tedy především o matematické analýzy vztahu mezi relativní frekvencí a velikostí útoků, které opět směřují k tomu, že i v kyberprostoru lze jejich distribuci vyjádřit pomocí mocninných zákonů (viz Maillart – Sornette 2010, Bibighaus 2015, Kuypers – Maillart – Paté-Cornell 2016).

Ve všech dílčích kombinacích oblastí zájmu (kybernetická bezpečnost, terorismus) a metod (systémová dynamika, mocninné zákony) již probíhá aktivní výzkum, je čím se inspirovat a na co navazovat. Tato práce je ale první, která kombinuje všechny tyto čtyři aspekty v jeden kvantitativní a simulovatelný model.

6 Referenční vzorek teroristických útoků

K posouzení, zda je model schopen replikovat historické chování systému, je využito údajů o džihádistických teroristických útocích, které na Západě (viz kapitola 4.3) proběhly od počátku roku 2007 do konce roku 2016. Kromě časového, geografického a ideologického omezení je doplňujícím kritériem také úspěšnost útoku. Z výzkumu byly vyřazeny útoky, které byly předem zmařeny anebo selhaly takovým způsobem, že nedošlo ke ztrátám na životech ani k žádným zraněním u nikoho kromě útočníků samotných (tj. včetně ozbrojených složek). Vzhledem k nulovým obětem nemají tyto teroristické útoky při modelování systému významnou roli.[57]

Jako primární zdroj byla použita globální databáze terorismu (*Global Terrorism Database,* GTD), kterou spravuje americká *University of Maryland* v rámci svého programu *Study of Terrorism and Responses to Terrorism*, který provozuje ve spolupráci s *U.S. Department of Homeland Security.* Tato databáze, jejíž první verze vznikla v roce 2001, obsahuje útoky z celého světa od roku 1970 a celkem obsahuje přes 170 tisíc položek (START 2017).

Z této databáze byla převzata data pro roky 2007 až 2015.[58] Z původní množiny necelých 90 tisíc útoků, které spadají do tohoto časového rozmezí, byly nejdříve odfiltrovány a vyřazeny všechny ty, které proběhly v jiných zemích, než na které se model zaměřuje. Poté následovalo postupné vyřazování útoků motivovaných jiným ideologiemi – především extrémní levicí (například v Řecku) a pravicí (žhářské útoky v Německu), etnoteritoriálními konflikty (na Korsice a Sardinii) nebo jinými náboženstvími (například křesťanský fundamentalismus v USA). Z této podmnožiny byly odstraněny útoky bez obětí (viz výše) a posledním krokem bylo manuální projití všech zbývajících teroristických útoků a vyřazení těch, které nebylo možné poloautomaticky odfiltrovat pomocí jejich parametrů v databázi – například antisemitské útoky.

V případě nejasností nebo rozporů sloužila jako sekundární zdroj podobná databáze od společnosti RAND (*RAND Database of Worldwide Terrorism Incidents*, RDWTI) a publicistické i oficiální informace vztahující se k jednotlivým útokům. Zařazení útoku k džihádismu bylo

---

[57] Příkladem takového nezdařeného útoku bez obětí může být třeba ten z 19. června 2017, kdy útočník v Paříži narazil automobilem naloženým výbušninami do policejní dodávky. K explozi ale nedošlo a při nárazu nebyl zraněn nikdo kromě tohoto sebevražedného řidiče (Samuel 2017). I pouhé zranění alespoň jednoho z přítomných policistů by ale vedlo k zařazení tohoto útoku do výzkumu (pomineme-li datum).

[58] Nyní GTD obsahuje i data pro rok 2016, ale aktualizace, která tato data přidala, byla vydána zhruba až v polovině července 2017, tedy příliš pozdě na to, aby mohla být zpracována a použita v modelu.

posuzováno především na základě kombinace několika faktorů: příslušnosti útočníků k nějaké známé organizaci, deklaraci jejich loajality k ní, přihlášení se k útoku ze strany džihádistické teroristické organizace a prohlášení vyšetřovatelů o charakteru a motivaci daného útoku.

Stejným způsobem a na základě stejných kritérii byly posléze doplněny i útoky za rok 2016, akorát na místo jediného hlavního a v relativně autoritativního zdroje musely být údaje k jednotlivým teroristickým útokům vyhledány a vyhodnoceny postupně (primárně dle Vidio - Marone - Entemann 2017). Následující tabulka shrnuje všech 52 položek, které splňuji kritéria:

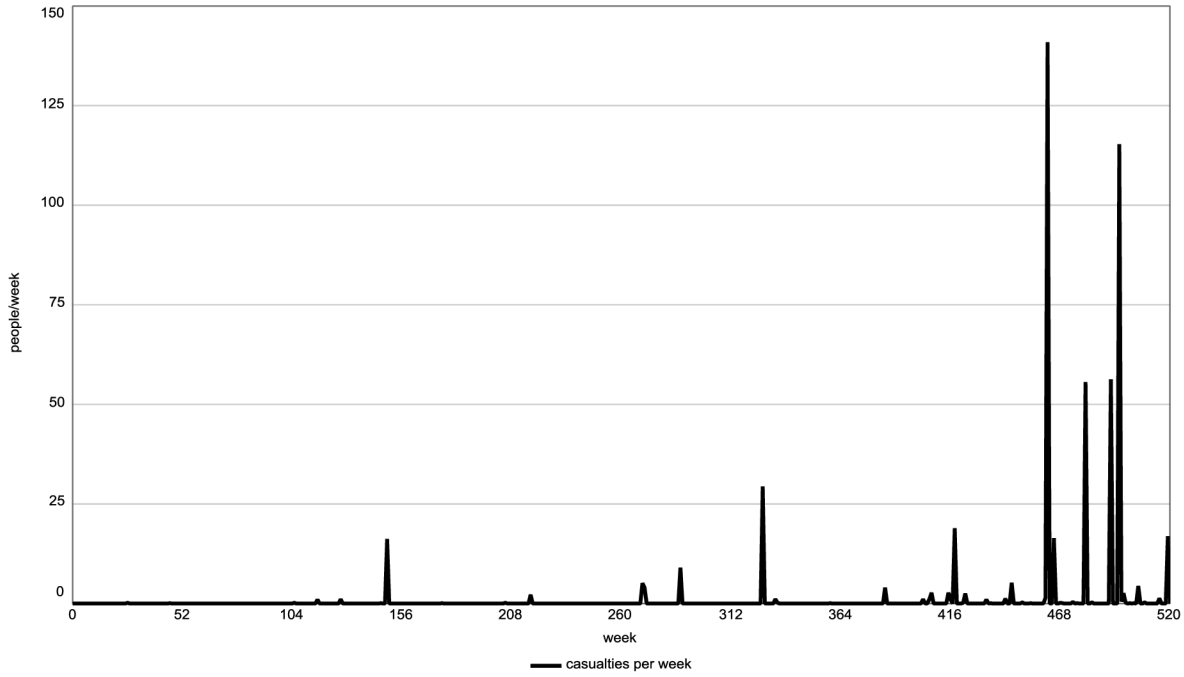
datum	týd	zab	zra	obětí	út	el	místo	typ útoku
2007-06-30	26	0	2	0.2	2	2	Glasgow, GBR	útok vozidlem
2007-11-12	46	0	1	0.1	1	0	Crissier, CHE	střelba
2008-12-31	105	0	2	0.2	1	0	Odense, DNK	střelba
2009-03-20	116	0	10	1	1	0	Lyon, FRA	střelba
2009-06-01	127	1	1	1.1	1	1	Little Rock, USA	střelba
2009-10-12	146	0	1	0.1	1	1	Milan, ITA	výbušnina
2009-11-05	149	13	32	16.2	1	1	Fort Hood, USA	střelba
2010-05-14	175	0	1	0.1	1	1	London, GBR	útok nožem
2010-12-11	205	0	2	0.2	1	0	Stockholm, SWE	výbušnina
2011-03-02	217	2	2	2.2	1	1	Frankfurt, DEU	střelba
2012-03-15	270	5	1	5.1	2	1	Toulouse, FRA + Brussels, BEL	střelba + žhářství
2012-03-19	271	4	0	4	1	0	Toulouse, FRA	střelba
2012-07-18	288	6	30	9	3	1	Burgas, BGR	výbušnina
2013-04-15	327	3	264	29.4	2	0	Boston, USA	výbušnina
2013-05-22	333	1	1	1.1	3	3	London, GBR + Paris, FRA	útok vozidlem + nožem
2013-05-26	334	0	2	0.2	3	3	Full Sutton, GBR	útok ve vězení
2013-11-18	359	0	1	0.1	1	1	Paris, FRA	střelba
2014-05-24	385	4	0	4	1	1	Brussels, BEL	střelba
2014-09-24	403	1	1	1.1	1	1	Moore, USA	útok nožem
2014-10-14	406	1	1	1.1	1	1	Quebec, CAN	útok vozidlem
2014-10-22	407	2	7	2.7	3	3	Ottawa, CAN + Quebec, CAN + New York, USA	střelba, útok vozidlem + sekerou
2014-12-20	415	2	7	2.7	2	1	Sydney, AUS + Joue-les-Tours, FRA	střelba + útok nožem
2014-12-21	416	0	11	1.1	1	1	Dijon, FRA	útok vozidlem
2015-01-07	418	17	19	18.9	3	3	Paris, FRA	střelba
2015-02-03	422	0	2	0.2	1	1	Nice, FRA	útok nožem
2015-02-14	423	2	5	2.5	1	1	Copenhagen, DEN	střelba

datum	týd	zab	zra	obětí	út	el	místo	typ útoku
2015-04-19	433	1	0	1	1	1	Paris, FRA	střelba
2015-05-03	435	0	1	0.1	2	2	Garland, USA	střelba
2015-06-26	442	1	2	1.2	1	1	Saint-Quentin-Fallavier, FRA	útok nožem
2015-07-16	445	5	2	5.2	1	1	Chattanooga, USA	střelba
2015-08-21	450	0	3	0.3	1	1	Arras, FRA	střelba a nůž
2015-09-17	454	0	1	0.1	1	0	Berlin, DEU	útok nožem
2015-11-02	461	1	4	1.4	2	2	Parramatta, AUS + Merced, USA	střelba + útok nožem
2015-11-13	462	128	129	140.9	9	6	Paris, FRA	střelba, výbušniny
2015-12-02	465	14	24	16.4	2	2	San Bernardino, USA + London, GBR	střelba + útok nožem
2016-01-01	468	0	2	0.2	1	1	Valence, FRA	útok vozidlem
2016-01-07	469	0	1	0.1	1	1	Paris, FRA	výbušnina
2016-02-11	474	0	4	0.4	1	1	Columbus, USA	útok mačetou
2016-02-26	476	0	1	0.1	1	1	Hanover, DEU	útok nožem
2016-03-22	480	32	236	55.6	5	3	Brussels, BEL	výbušniny
2016-04-16	483	0	3	0.3	3	0	Essen, GER	výbušnina
2016-06-12	492	51	53	56.3	2	2	Orlando, USA + Magnanville, FRA	střelba + útok nožem
2016-07-14	496	85	303	115.3	1	1	Nice, FRA	útok vozidlem
2016-07-18	497	0	5	0.5	1	1	Wurzburg, DEU	útok sekerou
2016-07-24	498	1	16	2.6	3	3	Ansbach, DEU + Saint-Etienne-du Rouvray, FRA	výbušnina + útok nožem
2016-08-06	499	0	2	0.2	1	1	Charleroi, FRA	útok mačetou
2016-08-19	501	0	1	0.1	1	1	Strasbourg, FRA	útok nožem
2016-08-30	503	0	1	0.1	1	1	Toulouse, FRA	útok nožem
2016-09-17	505	0	44	4.4	2	1	St. Cloud, USA + New Jersey, USA	útok nožem + výbušniny
2016-10-05	508	0	3	0.3	1	1	Brussels, BEL	útok nožem
2216-11-28	515	0	13	1.3	1	1	Columbus, USA	vozidlem a nožem
2016-12-19	519	12	49	16.9	1	0	Berlin, DEU	útok vozidlem

Tabulka 1 – přehled teroristických útoků zahrnutých do výzkumu

Protože časové rozlišení modelu je jeden týden, jsou všechny teroristické útoky, které proběhly v tom samém týdnu, sdruženy v jedinou položku. Z pohledu modelu a simulace tedy není rozdíl mezi tím, když v jednom týdnu proběhnou čtyři teroristické útoky po pěti obětech, nebo jediný útok s dvaceti oběťmi. To znamená, že za jeden útok nejsou považovány jen sousledné a koordinované útoky (například ty v Bruselu v roce 2016, nebo v Paříži v listopadu 2015), ale i ty, které proběhly s několikadenním zpožděním a v různých státech. Toto zjednodušení reflektuje i tabulka.

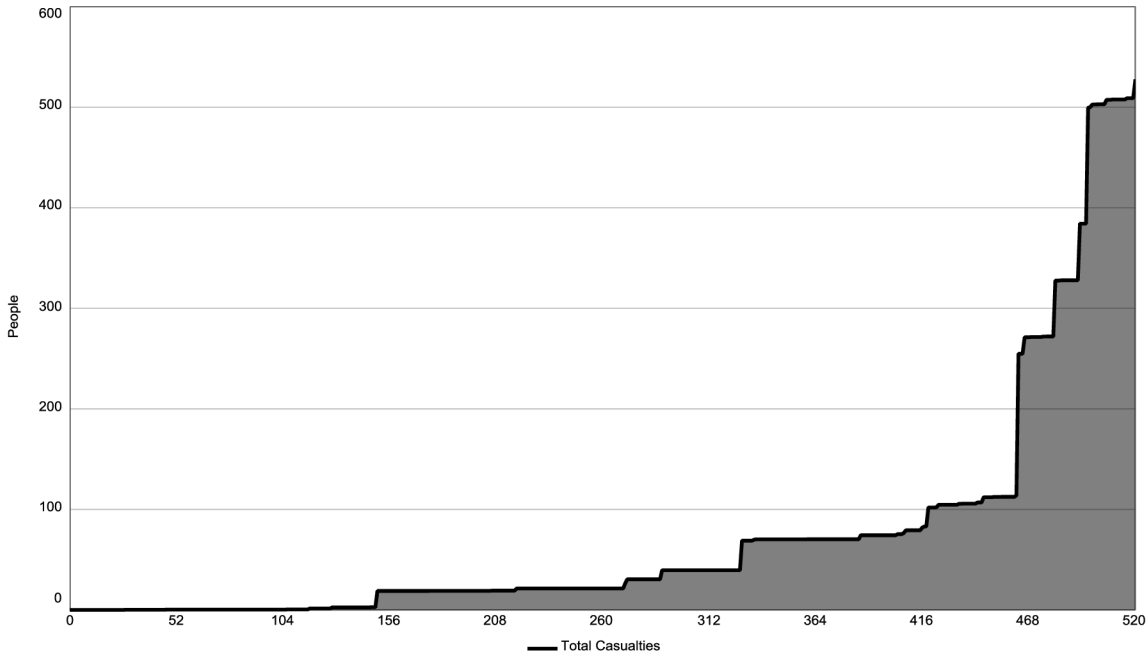
Zleva doprava sloupce ke každému útoku obsahují: datum; pořadí týdne, ve kterém útok proběhl; počet zabitých lidí; počet zraněných lidí; přepočítaný počet obětí (viz kapitola 4.3); počet útočníků přímo se podílejících na útoku; počet eliminovaných útočníků (jakýmkoliv způsobem zabitých, zraněných či zatčených, přičemž tento počet není nikdy obsažen v předchozích počtech zabitých ani zraněných lidí); místo, kde k útoku došlo; a nakonec typ útoku. Poslední dvě kategorie slouží spíše pro ilustraci a doplnění informací, neboť tento typ dat do modelu zahrnut není. V příloze se navíc nachází i korespondující tabulka, která obsahuje odkazy na zdroje (převážně publicistické) popisující konkrétní teroristické útoky.



Graf 11 – průběžný graf obětí džihádistických teroristických útoků za týden během let 2007-2016 (520 týdnů)

Tato data, respektive jejich část, lze zobrazit i v grafu (č. 11). Zde je zachycen vývoj spočítaných obětí (vertikální osa) džihádistických teroristických útoků pro jednotlivé týdny (horizontální osa). Na takto zobrazeném průběhu celých deseti let je nedávná eskalace, ke které došlo mezi lety 2014 a 2015, velmi dobře viditelná.

Alternativně lze ten samý trend zobrazit kumulativním grafem (č. 12), který zachycuje rostoucí počet celkových obětí. Akcelerace kumulace obětí je i zde dobře patrná.



Graf 12 – kumulativní graf obětí džihádistických teroristických útoků během let 2007-2016

Přestože se nejedná o jeden z deklarovaných cílů této práce, lze těchto dat využít i ke krátkému (a relativně povrchnímu) prozkoumání vlastností teroristických útoků. Nevyužití již dostupných a utříděných dat k alespoň zběžnému náhledu by bylo promarněnou příležitostí. Nejzajímavější poznatky lze získat rozdělením vzorku dle typu útoku. Ty jsou v tabulce 2[59] opět rozlišovány čtyři: útoky motorovými vozidly, útoky střelnými zbraněmi, útoky improvizovanými výbušninami a útoky chladnými zbraněmi.

Ještě před interpretací této tabulky je nutné upozornit na omezení, která plynou z povahy zdrojových dat, jejichž struktura vnáší jistá zkreslení. Hlavní zkreslení plyne z faktu, že některé útoky lze přiřadit k více typům. Běžně se vyskytují útoky kombinující typy zbraní, někdy i více než dvě. Útočníci mohou útok zahájit detonací podomácku vyrobené výbušniny a následně zahájit střelbu z automatických zbraní. Nebo ve vozidle, kterým se pokusí někoho srazit, mohou vézt další zbraně. Toto samozřejmě platí i v případě, kdy dochází k souběžným koordinovaným útokům. A

[59] "Sum" značí celkový počet pro danou kategorii, "%" značí její percentuální zastoupení a "avg" značí aritmetický průměr. "Poměr za/zr" vyjadřuje poměr mezi zabitými a zraněnými oběťmi pro konkrétní typ útoku a "el/út" vyjadřuje kolik procent útočníků je při daném typu útoku průměrně eliminováno (tj. zabito nebo zadrženo).

v tomto konkrétním případě je toto zkreslení ještě dále posilněno tím, že útoky jsou sdruženy po týdnech. K problému zde bylo přistupováno tak, že všechny oběti z daného týdne byly přiřazeny k tomu typu útoku, který jich způsobil nejvíce. Vzniká tak zkreslení, které posiluje efektivní metody útoků na úkor těch méně efektivních.

typ útoku	výskyt		zabití			zranění			poměr za/zr	útočníci		elim.		el/út
	sum	%	sum	%	avg	sum	%	avg		sum	avg	sum	avg	%
vozidla	8	15	99	25	12.4	382	29	47.8	3.9	11	1.4	10	1.3	0.91
střelba	22	42	252	64	11.5	304	23	13.8	1.2	40	1.8	31	1.4	0.78
IED	9	17	42	11	4.7	597	46	66.3	14.2	21	2.3	10	1.1	0.48
nože	13	25	2	1	0.2	26	2	2.0	13.0	15	1.2	14	1.1	0.93

Tabulka 2 – vlastností džihádistických teroristických útoků utříděných dle typu

Dalším problémem je poměrně malý vzorek, kdy u některých typů je méně než 10 případů a navíc jsou velmi nekonzistentní. To nejvíce dopadá na útoky vozidly (hlavně kvůli tomu v Nice ze 14. 7. 2016) a útoky improvizovanými výbušninami. Posledním zásadním problémem jsou chybějící neúspěšné útoky. I přes tato omezení snad lze tyto doplňující ilustrativní informace považovat za zajímavé a užitečné.

Z dat je patrné, že nejvíce obětí mají na svědomí útoky využívající střelné zbraně a zároveň patří k těm nejobvyklejším. Jako celkově nejnebezpečnější však vycházejí útoky využívající vozidla, které v průměru způsobily o jednoho zabitého více. Útoky chladnými zbraněmi (nože, sekery, mačety) jsou jednoznačně nejméně efektivní.

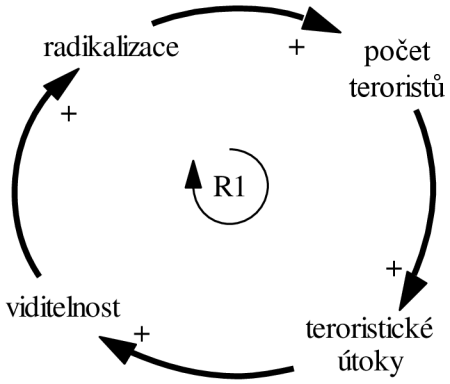
Snad až překvapivě velké rozdíly lze nalézt v kategorii zraněných. Zatímco útoky střelnými zbraněmi generují takřka vyrovnaný počet zraněných a zabitých, u improvizovaných výbušnin i chladných zbraní lze vidět obrovský nepoměr, až 14:1.

Pokud jde o charakteristiky vztahující se k útočníkům, i zde lze vidět markantní rozdíly. V prvé řadě útoky chladnými zbraněmi a vozidly jsou mnohem častěji individuální aktivitou, než je tomu u druhých dvou typů. Příčinami tohoto rozdílu jsou nejspíše dostupnost a nenáročnost těchto prostředků, takže k útoku není zapotřebí širšího zázemí, znalostí, prostředků ani kontaktů. U těchto dvou typů je zároveň velmi nízká pravděpodobnost (méně než 10%), že se útočníkům podaří uprchnout. Většina z nich při útoku zahyne nebo je zadržena. Naopak útočníci využívající výbušnin obvykle ani nejsou detonaci přítomni – výjimkou jsou samozřejmě sebevražedné útoky.

7 Model protidžihádistického vigilantismu v kyberprostoru

7.1 Konceptuální a kauzální struktura

Základem celé struktury je již výše zmíněná posilující zpětná vazba, která vychází z modelů od Pruyt – Kwakkel (2014) a Choucri et al. (2007). Tento cyklus (obr. 12) stojí na předpokladu, že provedené teroristické útoky zvyšují viditelnost ideologie, inspirují další sympatizanty, což zrychluje radikalizaci a zvyšuje počty potenciálních teroristů, kteří mohou provádět další teroristické útoky v budoucnu.[60]

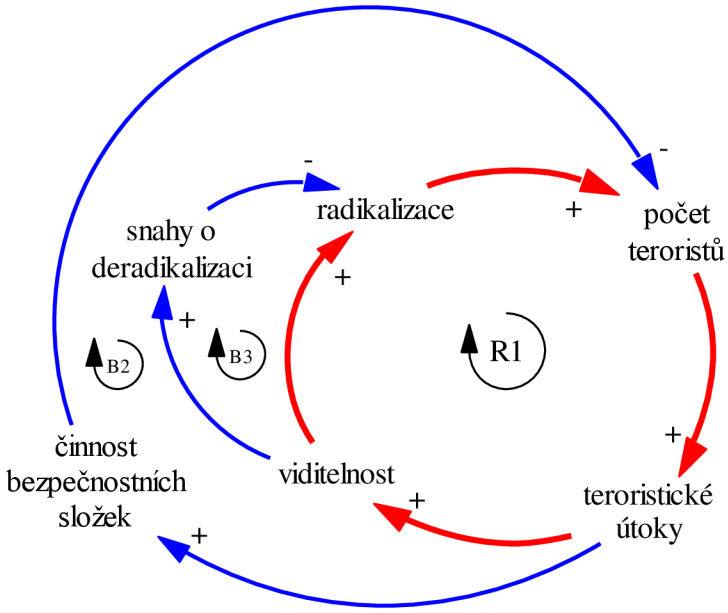


Obrázek 12 – základní diagram kauzálních smyček zpětné vazby mezi terorismem a radikalizací

Takováto posilující zpětná vazba (R1) by vedla k exponenciálnímu a ničím neomezenému růstu terorismu, přičemž je zřejmé, že realita je odlišná. Tento cyklus je totiž brzděn několika vyvažujícími zpětnými vazbami (obr. 13). Z pohledu státní moci a politického režimu lze identifikovat dvě základní činnosti, kterými na výskyt terorismu reaguje. Tou první jsou represivní bezpečnostní opatření (B2), kdy stát na teroristické útoky reaguje pomocí nasazení bezpečnostních složek (policie, armáda, zpravodajské služby, …), které mají za úkol tuto hrozbu co možná nejvíce minimalizovat, v ideálním případě zcela eliminovat skrze redukci počtu aktivních teroristů (během útoků i ještě před jejich zahájením). Druhým způsobem (B3) je snaha o co možná největší zbrzdění a v ideálním případě i zvrácení směru probíhajícího radikalizačního procesu (viz Milt et al. 2017,

[60] V zásadě se jedná o mechanismus velmi podobný původně anarchistickému konceptu "propagandy činem" (angl. *propaganda of the deed* nebo *propaganda by the deed*), kdy má odhodlaná avantgarda svými násilnými činy vyburcovat zbytek populace ke všeobecnému povstání a revoluci (Fleming 1980).

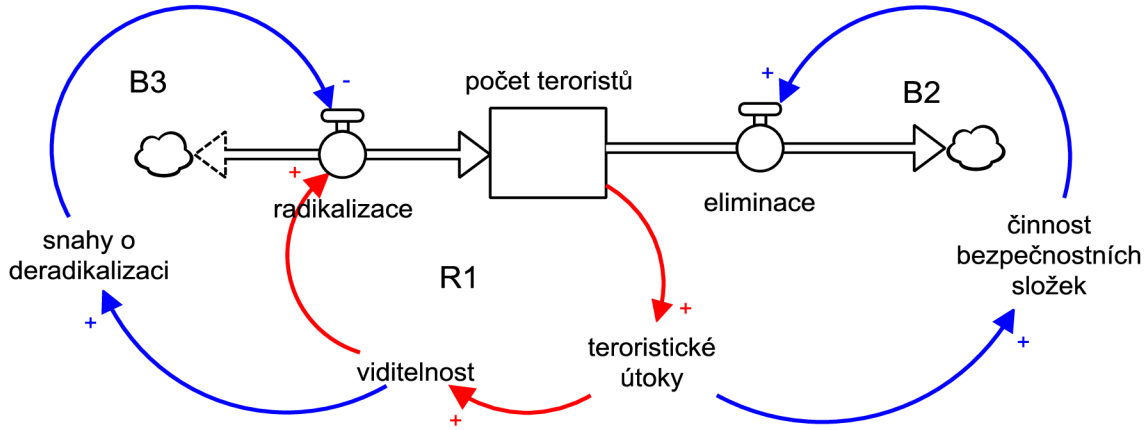
Reed 2017, Glazzard 2017). Posilující zpětná vazba je zaznačena červeně, vyrovnávající jsou modré.



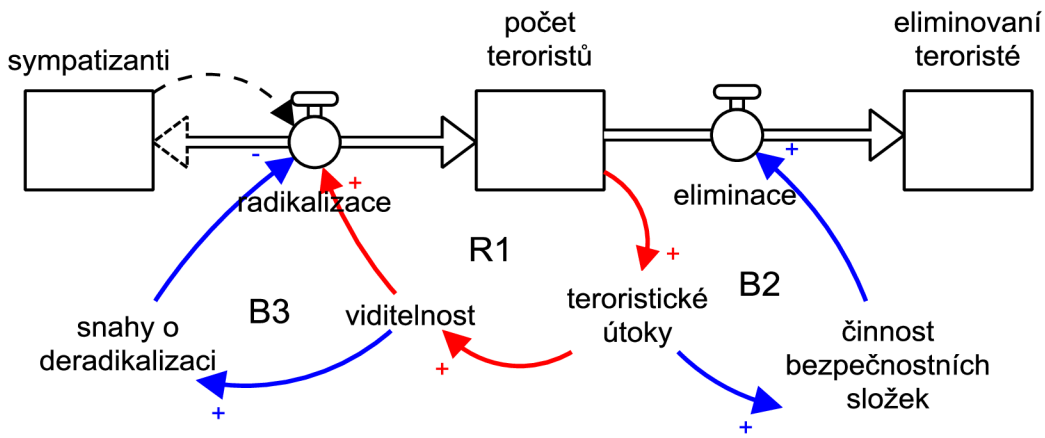
Obrázek 13 – diagram kauzální smyček terorismu s přidanými vyrovnávajícími zpětnými vazbami

K popisu těchto tří zpětných vazeb lze využít i přirovnání k již dříve popsanému fungování vany (viz kapitola 4.1.4). Počet teroristů si lze představit jako stav hladiny ve vaně, který je zvyšován radikalizací (přítok) a snižován jejich eliminací (odtok). Na vysokou hladinu, která se projevuje teroristickými útoky, reaguje stát snahou o zpomalení přítoku i zrychlení odtoku (obr. 14).[61]

[61] Zpětná vazba B2 je stále vyvažující, přestože v tomto diagramu má spoj jdoucí z "činnosti bezpečnostních složek" změněnou polaritu na kladnou. Důvodem je, že nyní směřuje do nově přidané proměnné „eliminace", která funguje jako odtok z hlavního stavu.

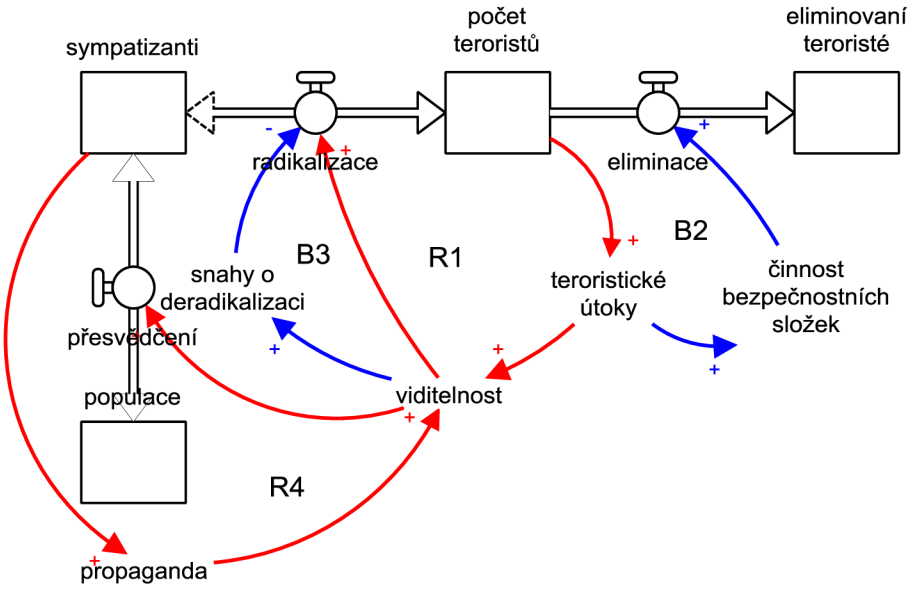


Obrázek 14 – smíšený kauzální diagram se stavy a toky pro eskalující terorismus a vyrovnávající zpětné vazby



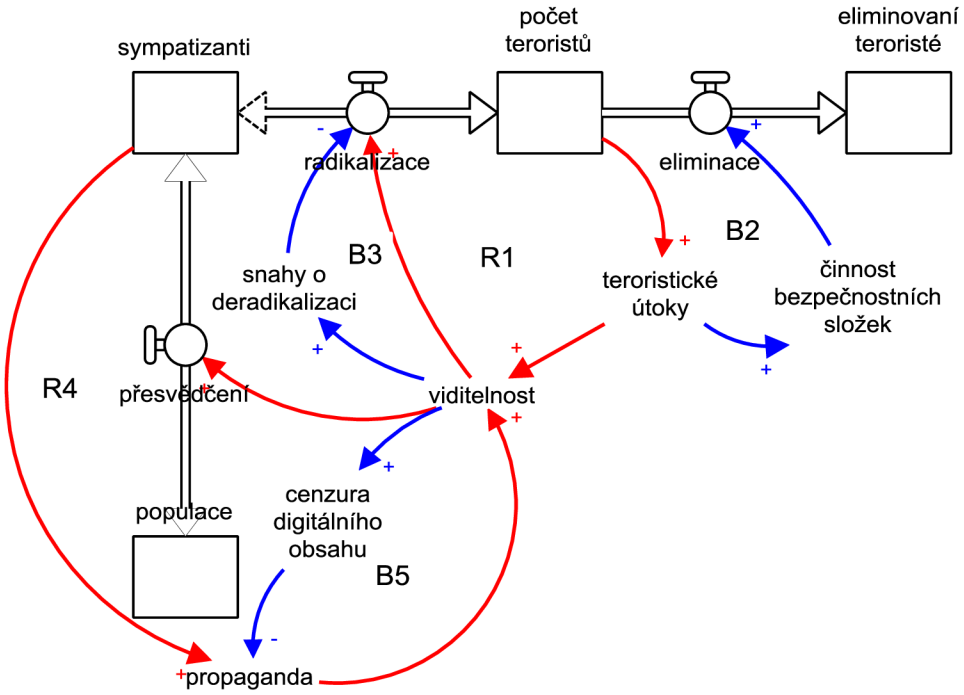
Obrázek 15 – smíšený diagram rozšířený o sousední stavy

Rozšířením hranice modelu (obr. 15) a přidáním obou sousedních stavů se objevuje další limitující faktor, který původní posilující se smyčku R1 zpomaluje. Zatímco akumulující se „eliminovaní teroristé“ na zbytek systému již nijak významně nepůsobí, tempo radikalizace je závislé na dostupné zásobě „radikalizovatelných sympatizantů.“ Počet teroristů tak nemůže exponenciálně a neomezeně růst už jen proto, že lidí, kteří by se teroristy vůbec mohli stát, není nekonečně mnoho. Diagram tak začíná nápadně připomínat model šíření nemoci skrze populaci (SIR), přičemž nakazitelní, nemocní a uzdravení lidé jsou nahrazení sympatizanty, aktivními teroristy a eliminovanými teroristy a vektorem šíření je namísto fyzického kontaktu násilná ideologie.



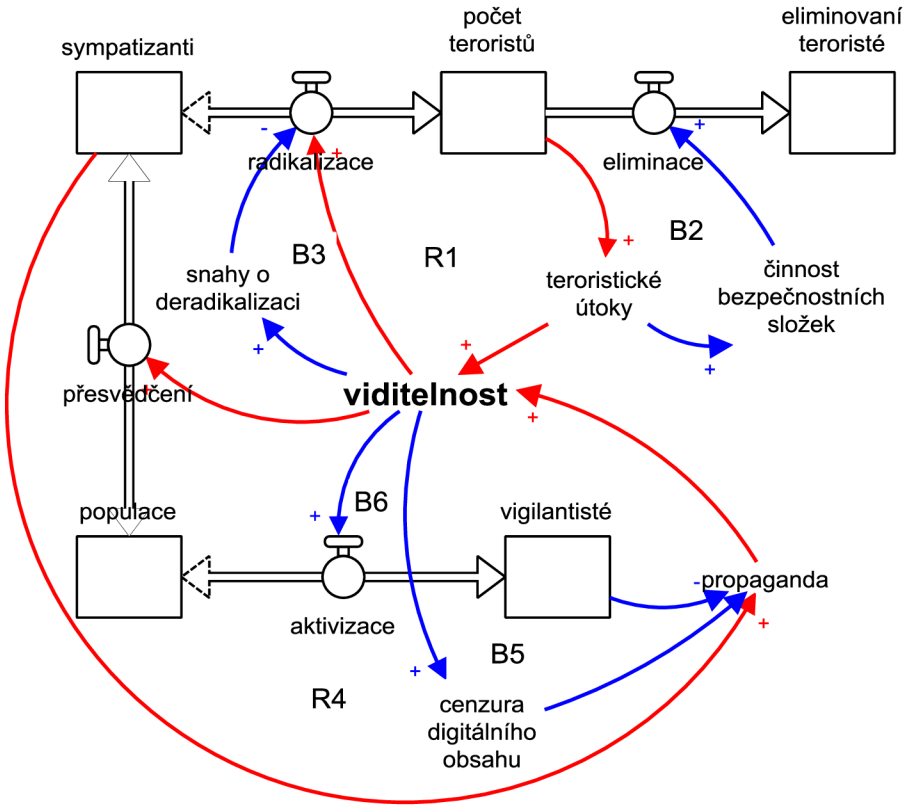
Obrázek 16 – smíšený diagram rozšířený o zpětnou vazbu nenásilné propagandy

Teroristické útoky však rozhodně nejsou jediným způsobem šíření těchto myšlenek. Vedle propagandy násilnými činy lze viditelnost ideologie zvyšovat i nenásilně. K tomu je dnes hojně využíváno právě elektronické komunikace a prostředí kyberprostoru (viz kapitola 3.1.1). Na těchto aktivitách se navíc může podílet daleko větší množství lidí, než kolik jich přikročí přímo k teroristickým útokům. Viditelnost tedy zvyšují i sami sympatizanti pomocí jimi šířené propagandy. Před sympatizanty lze navíc předřadit i další stav, který je reprezentován celkovou populací (obr. 16). Z tohoto stavu pak jde tok směrem k sympatizantům, jehož rychlost je ovlivňována viditelností a atraktivitou ideologie. Vzniká tak další posilující zpětná vazba, kdy vysoká viditelnost způsobuje nárůst počtu sympatizantů, kteří ji svojí činností zase zpětně zvyšují (R4).



Obrázek 17 – smíšený diagram rozšířený o zpětnou vazbu cenzury digitálního obsahu

Na tento proces reagují instituce a soukromé společnosti, jejichž platformy jsou k šíření propagandy využívány. Přímočarou a přirozenou reakcí je posílení regulačních mechanismů a cenzurování nežádoucího obsahu. I přestože je zavádění těchto nových mechanismů a pravidel velice problematické a pomalé (viz kapitola 3.4), vzniká tím nová vyvažující zpětná vazba B5, která brzdí a snižuje viditelnost džihádistické propagandy (obr. 17).

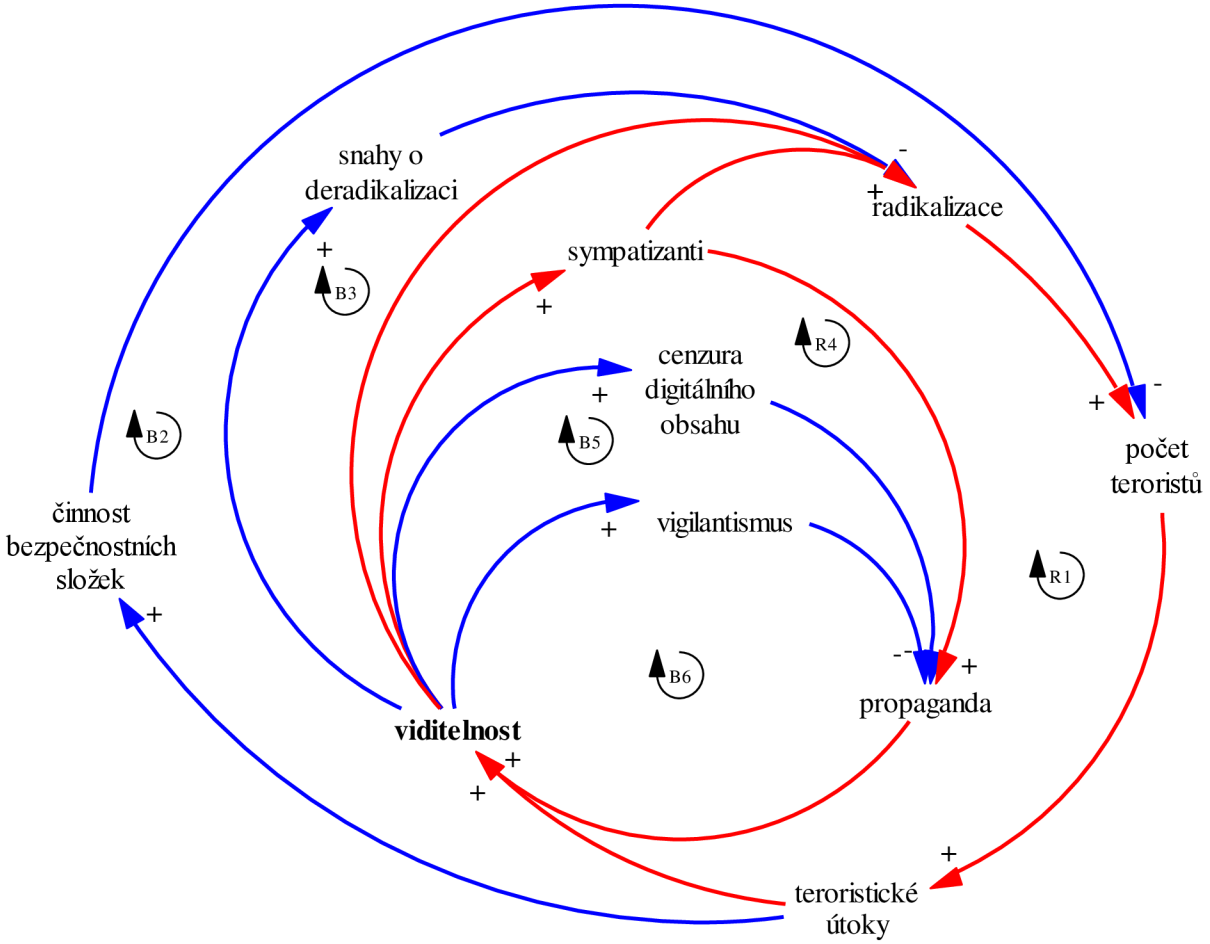


Obrázek 18 – finální smíšený kauzální diagram rozšířeny o zpětnou vazbu vigilantismu

Na dlouhé zpoždění a relativní neefektivitu regulace a cenzury tohoto obsahu reagují (mimo jiné) hacktivisté a vigilantisté (B6). Ti tak „berou spravedlnost do vlastních rukou“ a stavějí se do role, kdy dynamicky suplují činnost aktérů, kteří z jejich pohledu selhávají (viz kapitola 3.3). Agresivně (a často ilegálně) se zapojují do souboje o viditelnost džihádismu, kdy se ji snaží minimalizovat navzdory snahám přívrženců této ideologie o její co největší zviditelnění. Touto činností teoreticky brzdí jak akumulaci sympatizantů, tak jejich následnou radikalizaci. Viditelnost džihádismu (jeho ideologických principů a násilných i nenásilných aktivit jeho stoupenců) je tak základním kamenem celého systému i hlavním uzlem, v němž se střetávají protichůdné snahy dílčích subsystémů o její ovlivnění.

Bylo by možné dále pokračovat a do diagramu přidávat stále další a další prvky, nicméně již nyní se schéma začíná stávat relativně nepřehledným. Zvyšování podrobnosti by bylo spíše kontraproduktivní a už by nepřispívalo k lepší ilustraci základních vztahů mezi hlavními prvky systému a nejdůležitějšími zpětnými vazbami uvnitř něj.

Poslední krokem této kvalitativní části je rozvinutý diagram kauzálních smyček bez přidaných stavů a toků (obr. 19). Tento velice abstraktní a vysokoúrovňový náhled na systém tak zachycuje celkem šest zpětnovazebních smyček – dvě posilující R1 a R4, čtyři vyrovnávající B2, B3, B5 a B6. V tomto případě lze také všechny posilující zpětné vazby považovat za „nežádoucí“ z pohledu Západu a režimů čelících džihádismem motivovanému terorismu. Všechny vyrovnávající zpětné vazby působí přímo proti nim a terorismus i radikalizaci se snaží různými prostředky brzdit. Nelze ovšem analogicky tvrdit, že by všechny čtyři byly považovány za „žádoucí“, neboť přinejmenším vigilantismus (kvůli jeho ilegalitě a vedlejším obětem) a cenzuru (kvůli omezování svobody slova a rovněž nezamýšleným obětem) lze kritizovat. A i na tomto diagramu je vidět centrální role tučně zvýrazněné viditelnosti, kterou procházejí všechny zpětné vazby kromě B2, která spadá spíše do sféry vymáhání práva a pořádku (*law enforcement*) a tak reaguje přímo na násilné a jiné ilegální aktivity.

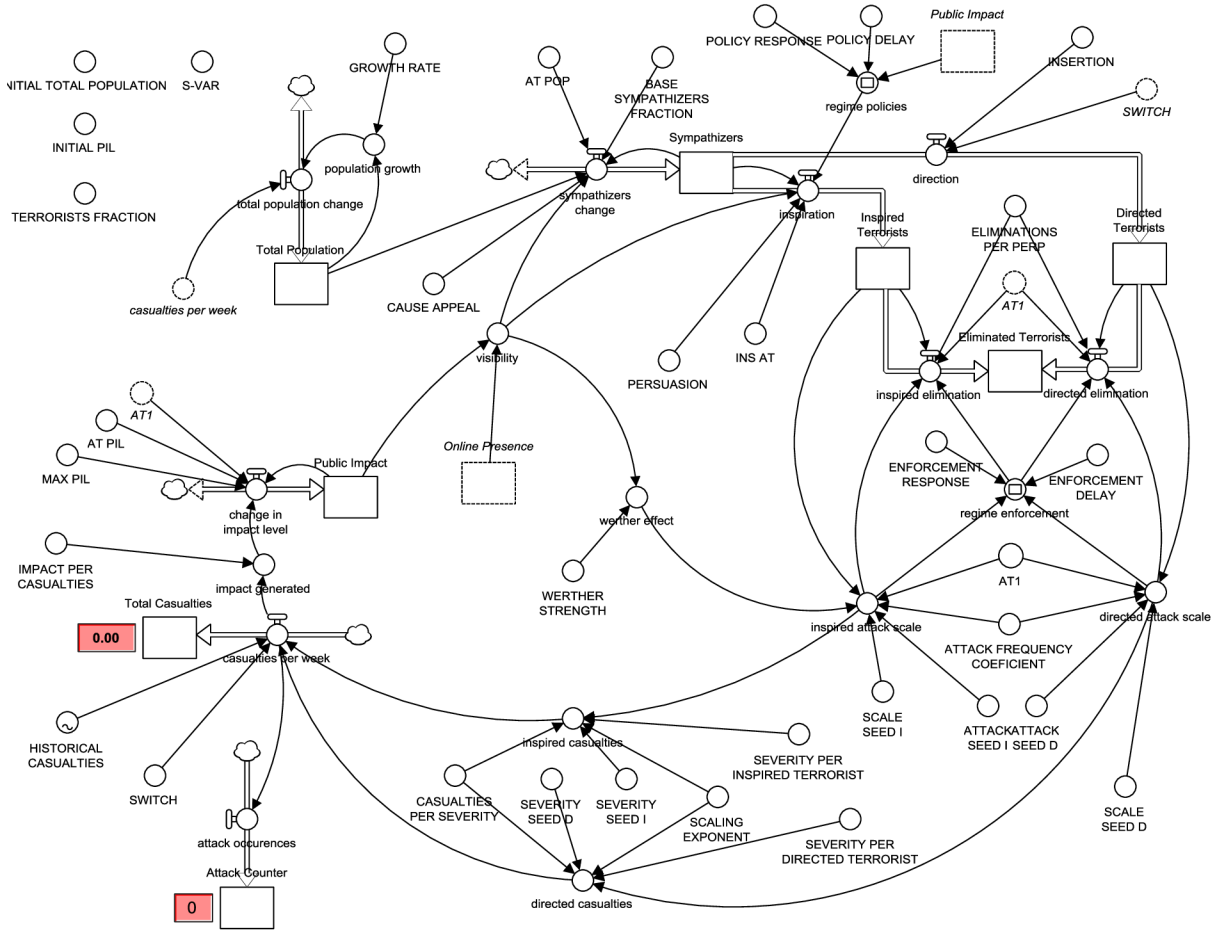


Obrázek 19 – finální diagram kauzálních smyček

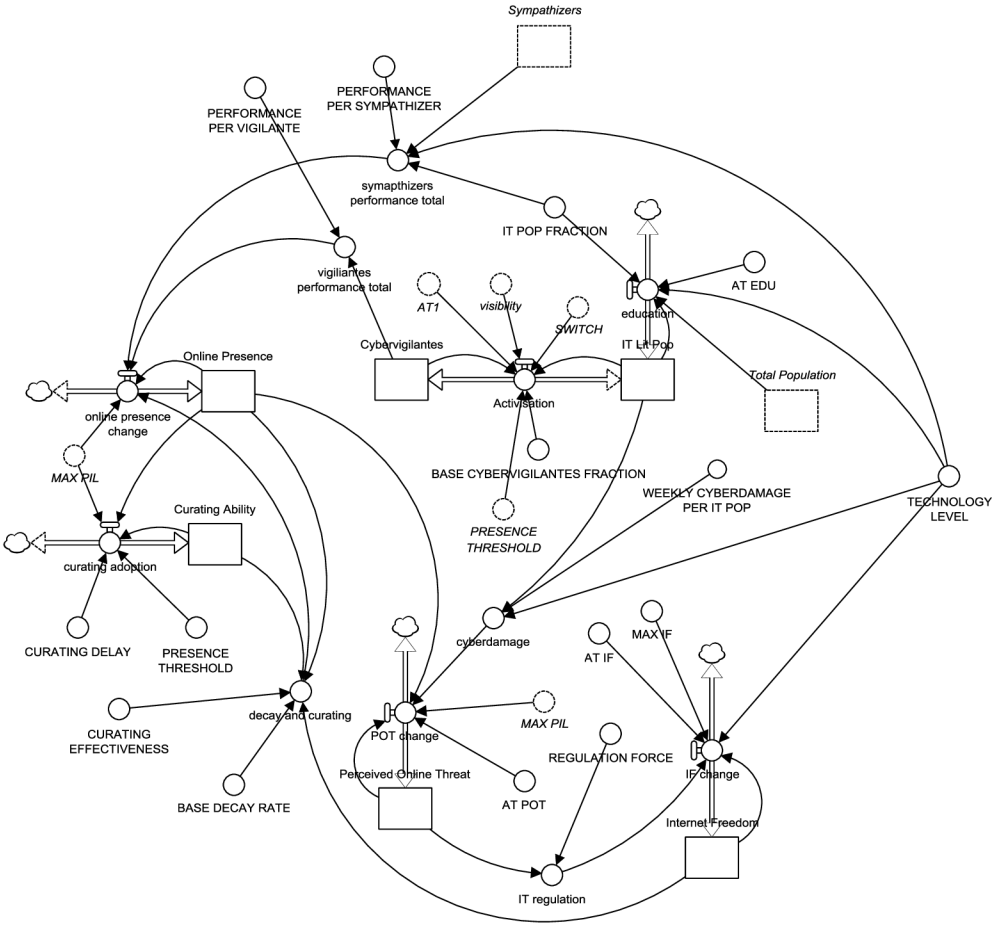
7.2 Matematická a logická struktura

Celý simulovatelný model se skládá ze dvou hlavních propojených částí. Obě poloviny jsou propojeny za pomocí tzv. zrcadlených či stínových proměnných, někdy označovaných i jako duchové (*shadow variable* nebo *ghost*). Ta první (obr. 20) zachycuje džihádistický terorismus jako takový a zaměřuje se na vývoj počtu teroristů, jejich sympatizantů, opatřeními ze strany režimu, generování teroristických útoků a jejich obětí a v neposlední řadě reakcemi, které tyto útoky ve společnosti vyvolávají.

V zásadě se tak jedná o mnohem detailnější ekvivalent předešlého jednoduchého diagramu na obrázku 13. Z hlediska uspořádaní na sebe jednotlivé části navazují následujícím způsobem ve směru hodinových ručiček od shora: sympatizanti – radikalizace – teroristické útoky – oběti útoků – viditelnost – sympatizanti.



Obrázek 20 – celkový diagram stavů a toků, první polovina



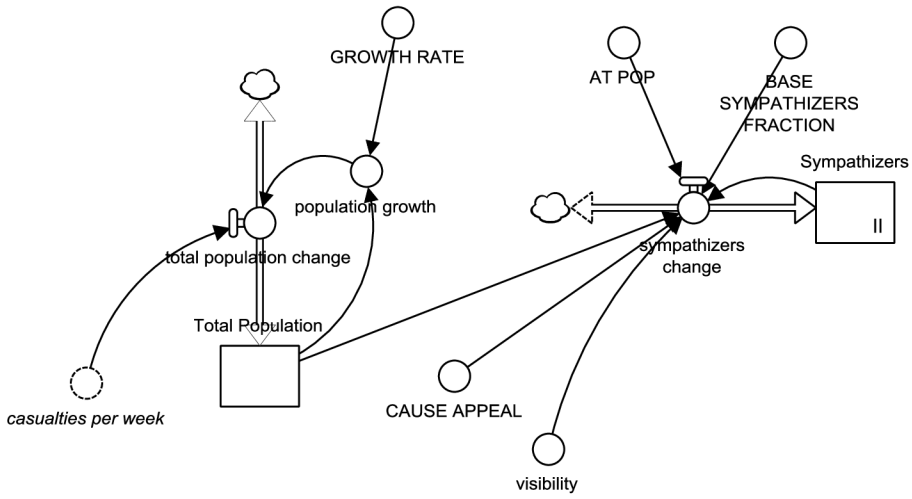
Obrázek 21 – celkový diagram stavů a toků, druhá polovina

Druhá funkční polovina modelu (obr. 21) zachycuje děje, které se odehrávají primárně v kyberprostoru. Ty se soustřeďují na ovlivňování viditelnosti džihádismu skrze sílu jeho přítomnosti v kyberprostoru, čímž je obecně myšlen obsah na webových stránkách, diskusních fórech, sociálních médiích atp. Řady sympatizantů a příznivců džihádismu se jeho přítomnost a viditelnost v kyberprostoru snaží navýšit, zatímco proti nim různou rychlostí a silou působí kybervigilantismus a cenzura.

Obě části jsou propojeny právě hlavně skrze výše zmiňovanou viditelnost, která je tím hlavním vstupem do druhé části modelu (společně s velikostí celkové populace a množstvím sympatizantů) a zároveň tím, na co tuto část modelu přímo působí.[62]

[62] V modelu nejsou reprezentovány snahy hacktivistů a kybervigilantistů o infiltraci džihádistických komunikačních kanálů a přímé maření plánovaných teroristických útoků skrze podávání takto získaných informacích bezpečnostním složkám (viz kapitola 3.3.1). Přestože by bylo technicky možné takovýto

7.2.1 Demografický segment



Obrázek 22 – diagram stavů a toků demografického segmentu modelu

Levá horní část modelu je v zásadě demografická a staví na datech Světové banky (World Bank 2017). Celková populace Západu (*Total Population*) začíná na 885 milionech a roste celkovým tempem 0.22% ročně[63] (*GROWTH RATE*) až na konečných 905 milionů v roce 2016. Pro úplnost je tento růst snižován o týdenní oběti teroristických útoků, i když v celkových počtech se jedná o takřka zanedbatelné množství. Výsledný vzorec růstu populace po dosazení konstant je:

```
total_population_change
      = population_growth - casualties_per_week
      = Total_Population * GROWTH_RATE - casualties_per_week
      = Total_Population * (0.0022/52.18) - casualties_per_week
```

Rovnice 1 – růst celkové populace

mechanismus do modelu zakomponovat, jedná se faktor, jehož síla není známá, neboť informace o této činnosti jsou velmi kusé, vágní, převážně nepotvrzené a nespolehlivé. Vzhledem k předpokládanému nízkému významu těchto aktivit a také nedostatku informací, na jejichž základě by bylo možné byť i slabý účinek rozumně odhadnout, je tento jev v modelu záměrně opomenut.

[63] Vzhledem k tomu, že základním časovým krokem v modelu je jeden týden, musí být i populační růst vyjádřen v procentech za týden. Roční populační růst je proto vydělen středním počtem týdnů v roce, což je, jsou-li v potaz vzaty i přestupné roky, ((365*3+366)/4)/7 = 52.18, tj. *GROWTH_RATE* = 0.0022/52.18.

Tok sympatizantů (*Sympathizers*) je oddělen a nevede přímo z celkové populace, takže potenciální sympatizanti jsou de facto součástí obou stavů. Rychlost tohoto toku závisí kromě celkové populace na viditelnosti džihádismu (*visibility*) a třech konstantách, z čehož jedna udává základní podíl této sekce populace (*BASE SYMPATHIZERS FRACTION*), rychlost změny (*AT_POP*) [64] a pomocné proměnné sloužící k vyrovnání jednotek. Výsledná rovnice růstu sympatizantů po dosazení konstant je:

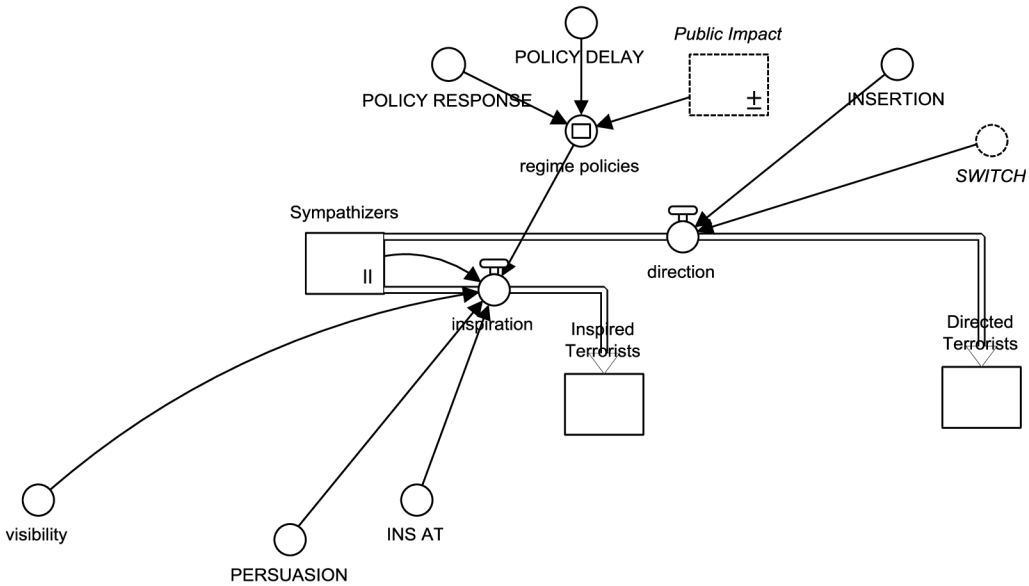
```
sympathizers_change
      = (CAUSE_APPEAL * Total_Population * visibility *
            BASE_SYMPATHIZERS_FRACTION - Sympathizers)/AT_POP
      = (1 * Total_Population * visibility *0.0013 - Sympathizers)/13
```

Rovnice 2 – změna množství sympatizantů

Při těchto parametrech model začíná s přibližně 230 tisíci sympatizanty. Na rozdíl od celkové populace nelze obecně stanovit konečný stav po deseti letech, neboť velice silně variuje mezi jednotlivými simulacemi v závislosti na generovaných teroristických útocích a výsledné viditelnosti a vnímané atraktivitě džihádismu. V podstatě se ale jedná o jednotky procent z celkové muslimské populace napříč celým Západem, přičemž odhad této hodnoty je notoricky obtížný, kontroverzní, nespolehlivý a dlouhodobě problematický (viz Sobolewska 2014 nebo Schmid 2017). S případným úspěchem snah o zviditelnění terorismu (násilně teroristickými útoky i propagandou v kyberprostoru) tento podíl pochopitelně roste.

[64] Zkratka "AT" v modelech systémové dynamiky obecně označuje "*Adjustment Time*", který se váže k rychlosti toků a rychlosti změny hladiny daného stavu. Jedná se tedy o časovou proměnnou, která určuje rychlost, respektive pomalost odezvy. Vyšší AT značí pomalejší tok a naopak.

7.2.2 Radikalizační segment



Obrázek 23 – diagram stavů a toků radikalizačního segmentu modelu

Dalším krokem je samotná radikalizace (obr. 23). Ta je tu rozdělena na dvě části dle typu teroristů a teroristických útoků z hlediska jejich organizovanosti (viz kapitola 3.1.2). Výsledkem jsou dva stavy, do kterých vedou toky od sympatizantů. Tím prvním stavem jsou inspirovaní teroristé (*Inspired Terrorists*), kteří sledují relativně tradiční cestu směrem k radikalizaci skrze ideologickou inspiraci a indoktrinaci. Tato skupina je sice mnohem méně organizovaná, navzájem nepropojená a logisticky v podstatě nepodporovaná, ale za to je mnohem početnější. Proces jejich radikalizace se se značným zpožděním snaží přímo brzdit vládní deradikalizační a protiteroristická politika (*regime policies*).

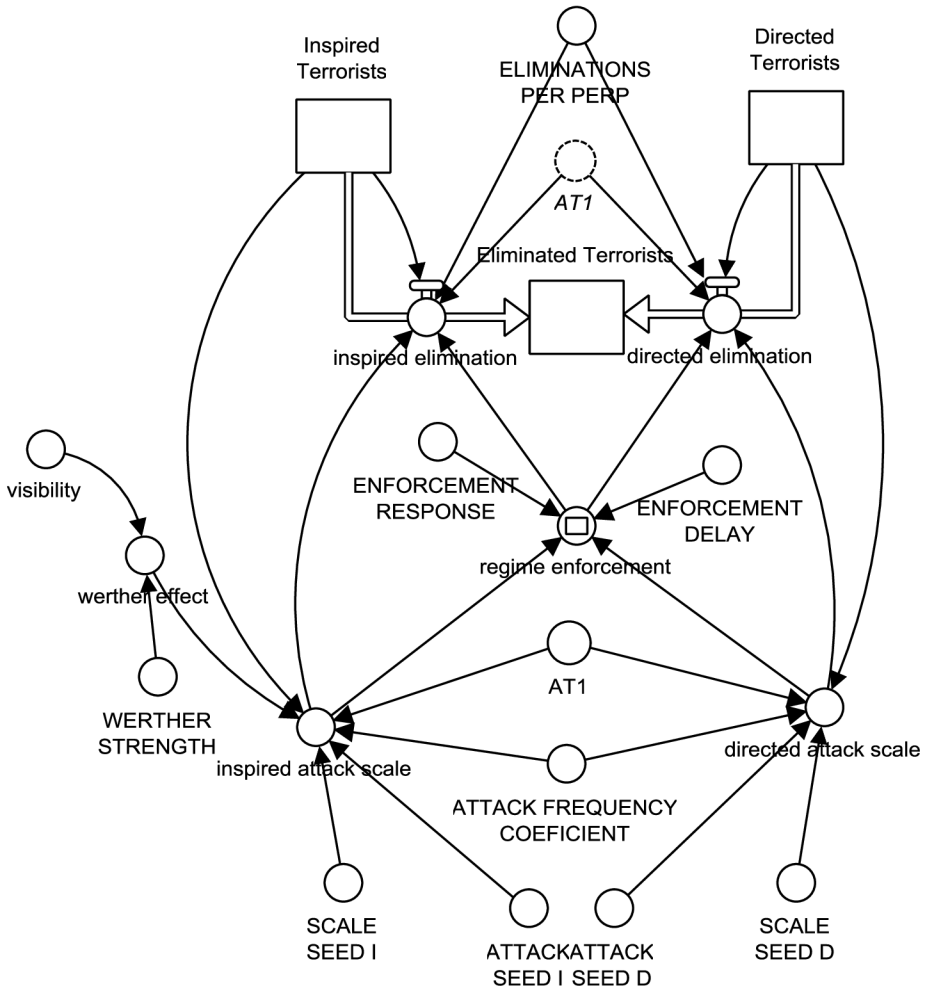
```
inspiration
      = Sympathizers * visibility * PERSUASION/
        (1 + regime_policies)/INS_AT
      = Sympathizers * visibility * PERSUASION/
        (1 + SMTH3(POLICY_RESPONSE*Public_Impact, POLICY_DELAY))/INS_AT
      = Sympathizers * visibility * 4e-6/
        (1 + SMTH3(0.1*Public_Impact, 208))/1
```

Rovnice 3 – radikalizace inspirací

Druhým stavem jsou řízení teroristé (*Directed Terrorists*), což jsou aktéři, kteří jsou přímo součástí nějaké teroristické organizace, jsou v kontaktu s dalšími buňkami a jsou dobře finančně i logisticky podporovaní. Zároveň jsou ale méně početní. Jedná se například o teroristy, kteří do cílových zemí přijíždějí ze zahraničních konfliktních oblastí, kde již podstoupili bojový a operační výcvik. Jsou tedy podstatně schopnější než jejich inspirované protějšky, a nepodléhají běžným radikalizačním ani deradikalizačním procesům, neboť do systému vstupují z vnějšku (v modelu skrze funkci *PULSE*). Jsou tedy modelováni jako externí vliv, který je do jinak relativně stabilního systému náhle vpuštěn a dává mu silný impuls ve formě malého počtu velmi motivovaných a schopných teroristů.

V tomto konkrétním případě se jedná o 21 lidí, kteří do systému vstupují v týdnu číslo 416, zatímco inspirovaných teroristů je v systému od samého počátku simulace asi 70 a jejich počet se dále odvíjí od úspěšnosti generovaných útoků a digitální propagandy, tj. analogicky se sympatizanty. Tyto přibližné odhady jsou založeny především na výročních zprávách Europolu o stavu a trendech terorismu v Evropské unii (TE-SAT: *European Union Terrorism Situation & Trend Report*, Europol 2007–2017) a publikacích Mezinárodního centra pro boj proti terorismu (ICCT: *The International Centre for Counter-Terrorism,* https://icct.nl/publications/) v Hágu (zejména van Ginkel - Entenmann 2016, Vidino - Marone - Entemann 2017). Zprávy TE-SAT jsou na numerická data nejbohatší, a i když interpretaci a extrapolaci těchto hodnot z EU na celý Západ komplikuje ne zcela konzistentní metodologie Europolu a jednotlivých členských států, jedná se o zdroj, který tuto obtížnou aproximaci umožňuje nejlépe. Posledním bodem, o který se lze opřít, jsou známé počty džihádistů, kteří se podíleli na teroristických útocích, které již proběhly (viz kapitola 6) nebo byly zmařeny.

7.2.3 Segment generující teroristické útoky



Obrázek 24 – diagram stavů a toků segmentu modelu generujícího teroristické útoky

Inspirovaní i řízení teroristé mají téměř identický mechanismus spouštění útoků, který závisí primárně na dvou pseudonáhodných hodnotách určujících, kdy k nim dojde (*ATTACK SEED*) a kolik teroristů se na nich bude podílet (*SCALE SEED*). Tyto hodnoty jsou v modelu zdvojeny a připojeny ke každému typu terorismu zvlášť, aby byly na sobě zcela nezávislé (viz obrázek 24). V okamžiku, kdy dojde k vygenerování hodnoty, která převyšuje koeficient odpovídající

historicky pozorované frekvenci útoků,[65] je útoku přidělen i počet útočníků,[66] který ovšem nemůže převyšovat celkový počet teroristů v daném zdrojovém stavu:

```
directed_attack_scale
      = IF (ATTACK_SEED_D > ATTACK_FREQUENCY_COEFICIENT)
            THEN MIN(SCALE_SEED_D, Directed_Terrorists)/AT1
            ELSE 0
      = IF ((RANDOM(0, 100) + 13) > 99)
            THEN MIN(SCALE_SEED_D, Directed_Terrorists)/1
            ELSE 0
```

Rovnice 4 – rozsah řízeného teroristického útoku

V tomto bodě spočívá hlavní rozdíl mezi oběma typy teroristických útoků v tom, že do spouštění útoků inspirovaných džihádismem vstupuje i dříve popisovaný „werther“ nebo „copycat“ efekt, který na krátkou dobu po kýmkoliv a jakkoliv provedeném džihádistickém útoku zvyšuje pravděpodobnost, že dojde k jeho impulzivnímu napodobení z řad snadno ovlivnitelných jedinců. Tento dynamický bonus zvyšující pravděpodobnost inspirovaného útoku v týdnech krátce následujících po významném zvýšení viditelnosti džihádismu je u řízeného terorismu kompenzován statickým zatížením celé pseudonáhodné funkce. Celá rovnice generující výskyt inspirovaných teroristických útoků a počet jejich účastníků vypadá i s dosazením konstant takto:

```
inspired_attack_scale
      = IF ATTACK_SEED_I > (ATTACK_FREQUENCY_COEFICIENT -
```

[65] Pro celých deset let běhu systému vychází tato zprůměrovaná historická hodnota na až podezřele kulatý desetitýdenní interval mezi jednotlivými útoky (ve vzorku je 52 útoků za 10 let). V průběhu prvních osmi let, tedy před eskalací, byla tato frekvence zhruba poloviční: 23 teroristických útoků za 8 let (tj. interval 18 týdnů). V posledních dvou sledovaných „post-eskalačních“ letech proběhlo celkem 29 útoků: jeden útok průměrně každého tři a půl týdne. Situaci by tedy šlo popsat tak, že mezi lety 2014 a 2015 došlo k více než zpětinásobení frekvence džihádistických teroristických útoků na Západě.

[66] Pseudonáhodné funkce určující počet útočníků jsou mezi oběma typy odlišné a jsou zvoleny tak, aby reflektovaly typicky pozorované počty teroristů účastnících se útoků dle referenčního vzorku. Velmi obecně lze říci, že inspirované útoky jsou častěji individuální záležitostí (částečně kvůli své relativní spontánnosti), zatímco ty řízené bývají spíše prováděny v malých týmech. K reprezentaci těchto distribucí byly iterativně zvoleny následující funkce:

$$\text{SCALE_SEED_I} = \text{ROUND}\left(\frac{1}{\sqrt[8]{\text{RANDOM}(0,1000)}} * 7\right) - 2 \;\; ;\text{SCALE_SEED_D} = \text{ROUND}\left(\frac{1}{\sqrt[2]{\text{RANDOM}(0,1000)}} * 42\right)$$

Ilustrativní grafy výstupu generovaného těmito dvěma zástupnými funkcemi lze nalézt v příloze.

```
                        werther_effect *
                        Inspired_Terrorists/SCALE_SEED_I)
        THEN MIN(SCALE_SEED_I, Inspired_Terrorists)/AT1
        ELSE 0
= IF ATTACK_SEED_I > (ATTACK_FREQUENCY_COEFICIENT -
                        visibility * WERTHER_STRENGTH *
                        Inspired_Terrorists/SCALE_SEED_I)
        THEN MIN(SCALE_SEED_I, Inspired_Terrorists)/AT1
        ELSE 0
= IF (RANDOM(0, 100)) > (99 -
                          visibility * 0.19 *
                          Inspired_Terrorists/SCALE_SEED_I)
        THEN MIN(SCALE_SEED_I, Inspired_Terrorists)/1
        ELSE 0
```

Rovnice 5 – velikost inspirovaného teroristického útoku

Posledním dějem probíhajícím v této části modelu je eliminace teroristů. Ta probíhá zcela symetricky, bez rozdílů pro oba typy terorismu a lze ji dále dělit na dva způsoby eliminace. Tou první je jejich eliminace přímo během teroristických útoků nebo okamžitě po nich (například během pokusu o únik), která je přímo úměrná počtu útočníků. Druhým způsobem je eliminace teroristů přímo z jejich stavu skrze průběžnou činnost bezpečnostních složek reprezentovanou proměnnou *regime enforcement*, která svým navýšením na útoky reaguje se zpožděním (byť čtvrtinovým oproti deradikalizační proměnné *regime policy*).

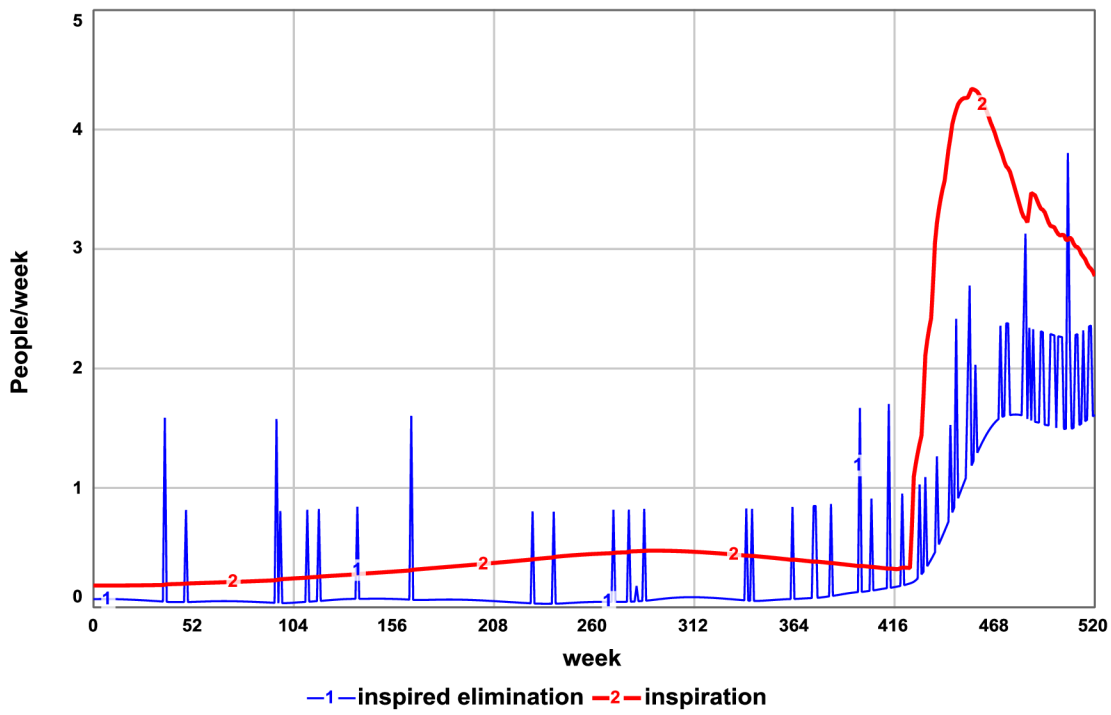
```
inspired_elimination
      = regime_enforcement
        * Inspired_Terrorists/AT1
        + inspired_attack_scale*ELIMINATIONS_PER_PERP
      = SMTH3((inspired_attack_scale + directed_attack_scale)
              * ENFORCEMENT_RESPONSE, ENFORCEMENT_DELAY, [init])
        * Inspired_Terrorists/AT1 +
        + inspired_attack_scale*ELIMINATIONS_PER_PERP
      = SMTH3((inspired_attack_scale + directed_attack_scale)
              * 0.01, 52, 0.001)
        * Inspired_Terrorists/1 +
        + inspired_attack_scale*0.77
```

Rovnice 6 – eliminace inspirovaných teroristů

Intenzita obou způsobů eliminace (respektive hodnota příslušných řídících parametrů), jak během útoků, tak mimo ně, je opět aproximována na základě historických dat. Hodnota 0.77 (tj.

77%) pro podíl teroristů zabitých přímo během útoku nebo okamžitě po něm vychází z referenčního vzorku a jedná se o jednoduchý aritmetický průměr všech jednotlivých poměrů mezi teroristy, kteří se útoku účastní a těmi, kteří jsou při něm nějakým způsobem eliminováni: $\sum_{n=1}^{n=52}\left[\frac{\text{útočníci}_n}{\text{eliminovaní útočníci}_n}\right]/52 = 0.77$. Počty teroristů zadržených či zabitých v rámci policejních operací, které nejsou bezprostřední reakcí na teroristický útok, jsou přibližně odhadnuty na základě zpráv TE-SAT (Europol 2007-2017).

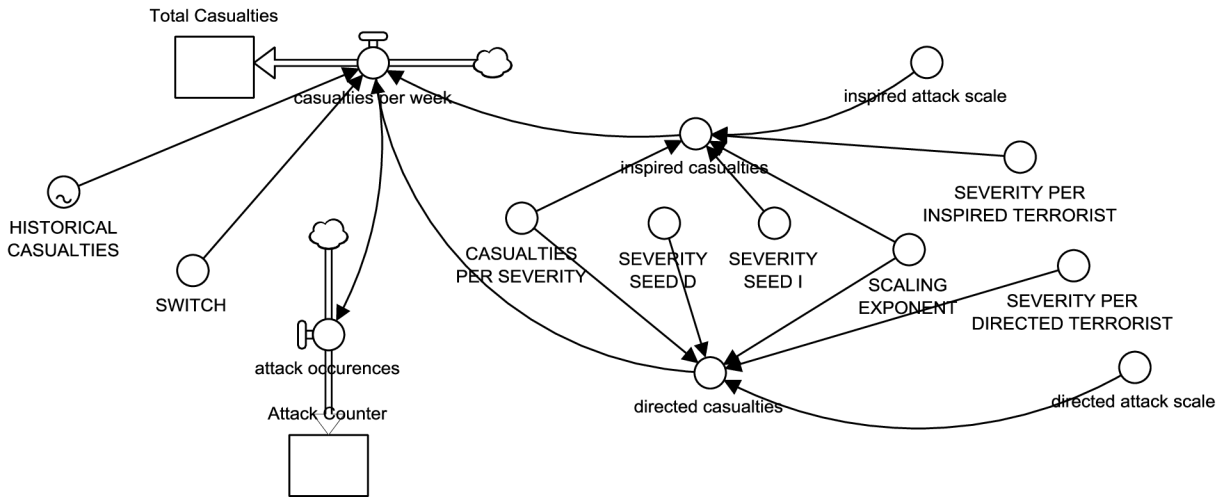
Souběžnou interakci mezi radikalizací (v modelu specificky „inspirací“) a eliminací lze zobrazit na grafu, který zachycuje oba dva toky v čase (graf 13). Jedná se o dynamicky vygenerovaný (tj. fiktivní) příklad. Jednotlivé vrcholky korespondují s okamžitou reakcí na teroristické útoky uvnitř systému, zatímco pod nimi lze vidět plynuleji se vyvíjející dlouhodobou odezvu, která ovšem (alespoň v tomto konkrétním simulovaném případě) zaostává za přítokem nových teroristů (jednotkou obou toků je člověk/týden).



Graf 13 – graf simulovaného přítoku a odtoku stavu inspirovaných teroristů

7.2.4 Segment generující oběti teroristických útoků

Čtvrtá část navazuje na vygenerované útoky a přiděluje jim počty obětí. Jedná se o klíčové místo, kde dochází k hlavnímu uplatnění mocninného zákona (viz kapitola 4.2) a i zde se nachází paralelní struktura rozlišující mezi inspirovanými a řízenými útoky i s duplikovanými generátory pseudonáhodných čísel. Je to také právě zde, kde dochází k rozlišení účinnosti obou typů útoků, neboť řízené teroristické útoky mají v průměru na svědomí mnohem větší množství obětí než ty inspirované (v modelu je to zhruba pětinásobek). Obě dvě funkce generující výsledné počty obětí tak mají stejný exponent a sklon, ale jsou „zatíženy“ odlišnými koeficienty, které přiřazují závažnost konkrétního útoku (v modelu pod jménem *SEVERITY*) podle počtu útočníků vygenerovaných v předchozím segmentu.



Obrázek 25 - diagram stavů a toků segmentu modelu generujícího oběti teroristických útoků

Celá rovnice generující počet obětí inspirovaného teroristického útoku vypadá i s dosazením konstant a funkce produkující pseudonáhodné číslo takto:

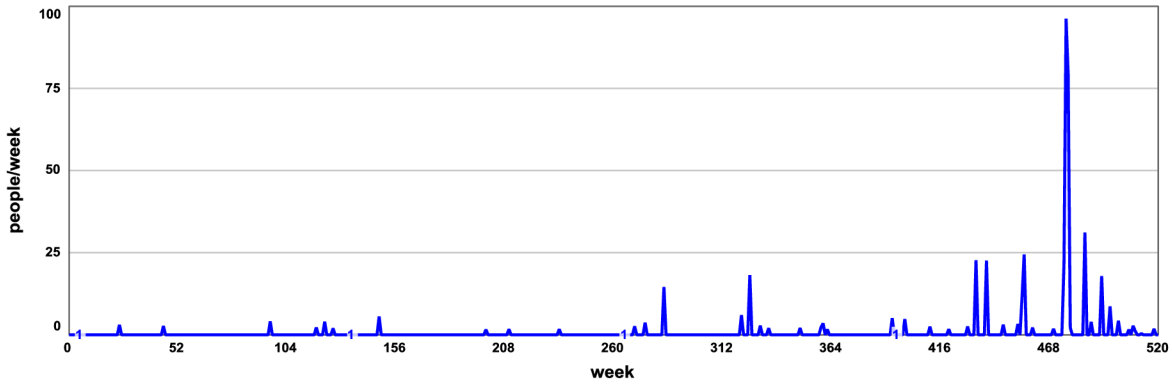
```
inspired_casualties
      = SEVERITY_PER_INSPIRED_TERRORIST * inspired_attack_scale *
        CASUALTIES_PER_SEVERITY * (1/SEVERITY_SEED_I)^(1/SCALING_EXPONENT)
      = 1.6 * inspired_attack_scale *
        1 * (1/ RANDOM(0, 1))^(1/ 2.02)
```

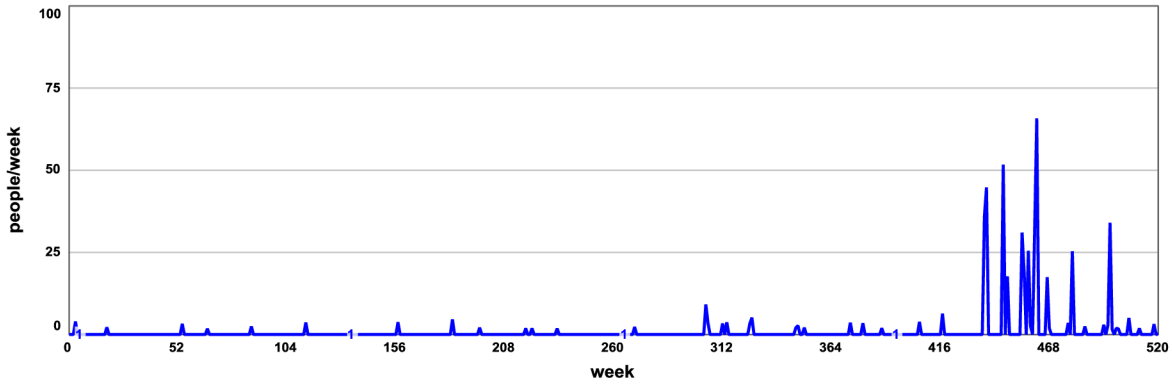
Rovnice 7 – kalkulace obětí inspirovaných teroristických útoků

Pro řízené útoky je rovnice zcela analogická a liší se jen tím, že používá svoje vlastní vstupy. V tomto segmentu modelu zároveň dochází i ke splynutí obou typů útoků v jediný výstup a tok obětí džihádistického terorismu. Tento tok (*casualties per week)* je jednoduchým součtem obou typů útoků a jeho jednotkou jsou lidé/týden. Směřuje do stavu, v němž dochází k postupné akumulaci všech obětí teroristických útoků, a který slouží primárně ke kontrolním a validačním účelům. Druhým takovým „diagnostickým počítadlem" je pomocný stav akumulující počet útoků, respektive týdnů, ve kterých k útokům došlo. Tento stav je podmínkovou funkcí jednoduše navýšen o 1 vždy, když počet obětí v daném týdnu překročí 0: `attack_occurences = IF (casualties_per_week>0) THEN 1 ELSE 0`.

Na diagramu je také vidět časová řada (reprezentovaná takzvanou grafickou funkcí, viz viditelná „vlnka" v symbolu proměnné) nazvaná *HISTORICAL CASUALTIES*, která, jak název napovídá, obsahuje historickou sekvenci obětí pro jednotlivé týdny let 2007 až 2016. Pomocí hned vedle umístěného přepínače *SWITCH* lze model jednoduše a rychle přepínat mezi chováním historickým a simulovaným, včetně několika dalších parametrů, jako například zda vůbec dojde ke vstupu řízených teroristů do systému. Celý model tak lze simulovat v několika různých módech, které lze navzájem porovnávat.

Simulované výstupy z tohoto segmentu lze demonstrovat na dvou příkladech, které zobrazují kombinovaný tok obětí obou typů teroristických útoků (grafy 14):

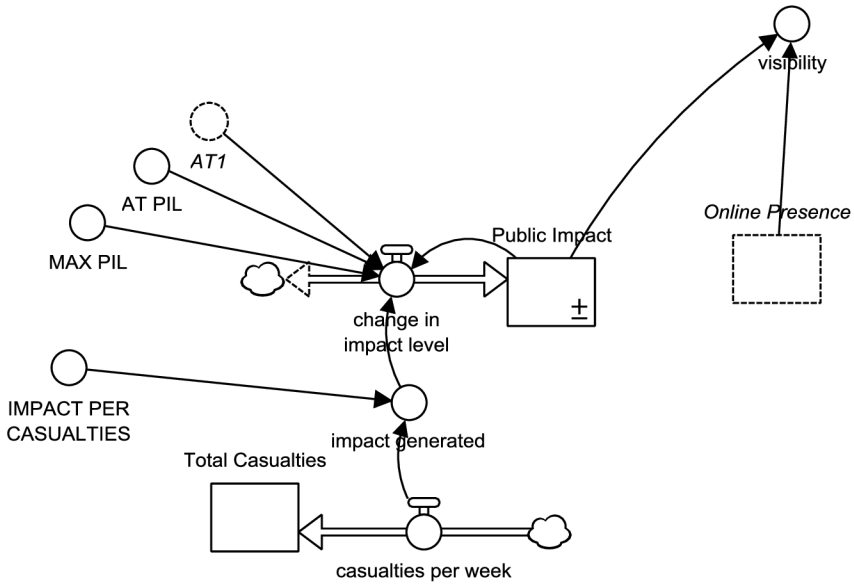




Grafy 14 - příklady počtů obětí simulovaných teroristických útoků uvnitř modelu

Při srovnání s historií (viz graf 11) lze rozpoznat velmi podobné obecné chování co do frekvence, rozložení i do velikosti jednotlivých útoků. Na druhou stranu je třeba upozornit, že přestože se jedná o jeho obvyklé chování, model místy generuje i zcela netypicky klidné nebo naopak excesivně aktivní simulace se zcela odlišným průběhem a útoky s mnoha sty obětí. V přílohách lze nalézt tři ukázky ze simulací, v jejichž průběhu došlo k více než tisíci obětí.

7.2.5 Segment generující viditelnost džihádismu



Obrázek 26 - diagram stavů a toků segmentu modelu generujícího viditelnost džihádismu

Poslední krokem k uzavření celého základního cyklu džihádistického terorismu je vyjádření jeho viditelnosti, které se zde skládá z přímého dopadu na veřejnost (*Public Impact*) a z digitální propagandy v kyberprostoru (*Online Presence*). Zdrojem dopadu na veřejnost jsou právě oběti teroristických útoků z předchozího segmentu. Tento stav má za cíl vyjadřovat pozornost, jaká je tomuto fenoménu věnována mezi lidmi, relativní saturaci tradičních médií a strach z terorismu, který ve společnosti panuje. Vzhledem k tomu, že tato proměnná není prakticky a snad ani teoreticky měřitelná, byla pro ni stanovena vlastní jednotka a spojitá škála od 0 do 1, přičemž 1 značí maximální možnou saturaci, strach a dopad na veřejnost.

Tato klíčová rovnice toku vychází z předpokladu, že tento dopad nových obětí terorismu na veřejnost není lineární a mění se v závislosti na stávajícím stavu. Jinak řečeno, reakce na ten samý útok bude odlišná, bude-li představovat izolovanou a jedinečnou událost, než když bude součástí kontinuální kampaně opakovaných útoků. Osamocený teroristický útok ve stabilní a „klidné“ společnosti obvykle nevyvolá tak silnou atmosféru strachu a pocitu ohrožení jako v té, která takovým útokům čelí pravidelně. Naopak je-li intenzita takové kampaně již velmi vysoká, společnost si „zvyká“, stává se odolnou (angl. *resilient*) a je čím dál těžší ji takto šokovat (viz Speckhard 2011: 15-1:15-10, Gal 2013, Elran 2017). Pro daný počet obětí je navýšení společenského dopadu tedy relativně nejvyšší, pokud je aktuální stav blízko u střední hodnoty,

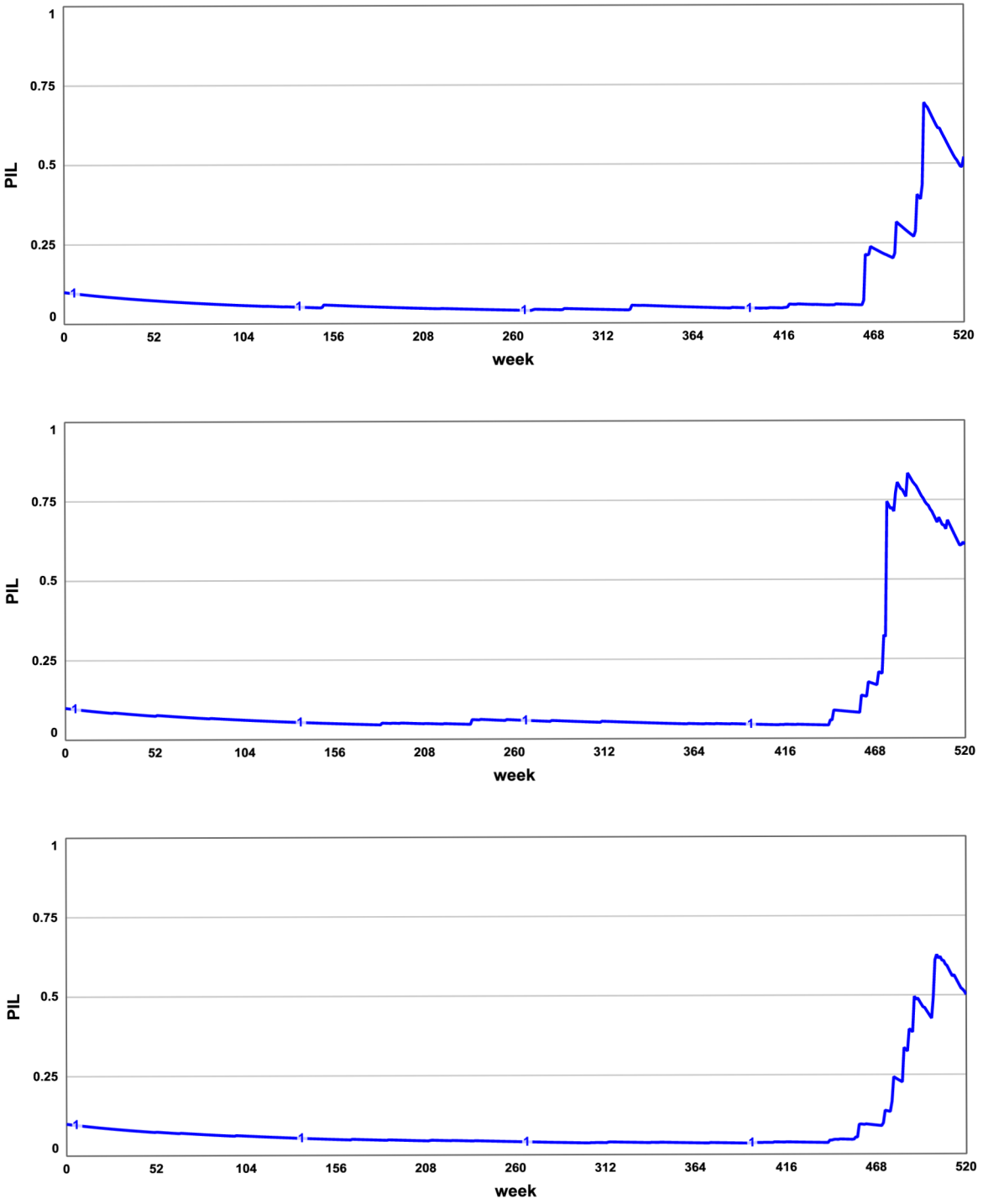
tedy ½. Čím blíže se hodnota nachází u jednoho z extrémů, k tím menší dojde změně a tím pomaleji se stav mění. Parametry modelu jsou kalibrovány tak, aby historické maximum produkovalo zhruba dvoutřetinovou hodnotu tohoto stavu, což časově koresponduje s útokem v Nice 14. července 2016.

Tato nelinearita je zprostředkována matematickou rovnicí, která konceptuálně vychází z proměnlivosti obsahu rovnoběžníků při zachování konstantního obvodu. Takový obsah je největší, právě když jsou obě strany stejné, přičemž zde jsou strany reprezentovány hladinou stavu *Public Impact* a zbytkem této hladiny, tj. *1 - Public Impact*. Součin těchto hodnot bude dosahovat maxima právě v polovině stavu (*0.5 * 0.5 = 0.25*) a postupně klesat s tím, jak se od středu bude vzdalovat (například *0.1 * 0.9 = 0.09*), a to i přestože součet obou imaginárních stran je zcela konstantní. Celá rovnice i s dosazením konstant vypadá následovně:

```
change_in_impact_level
      = MIN(
            (MAX_PIL-Public_Impact)/AT1,
            (impact_generated-Public_Impact) *
                  (Public_Impact * (MAX_PIL-Public_Impact))
                  /MAX_PIL^2/AT_PIL
          )
      = MIN(
            (MAX_PIL-Public_Impact)/AT1,
            (casualties_per_week*IMPACT_PER_CASUALTIES-Public_Impact) *
                  (Public_Impact * (MAX_PIL-Public_Impact))
                  /MAX_PIL^2/AT_PIL
          )
      = MIN(
            (1-Public_Impact)/1,
            (casualties_per_week*0.15-Public_Impact) *
                  (Public_Impact * (1-Public_Impact))
                  /1^2/13
          )
```

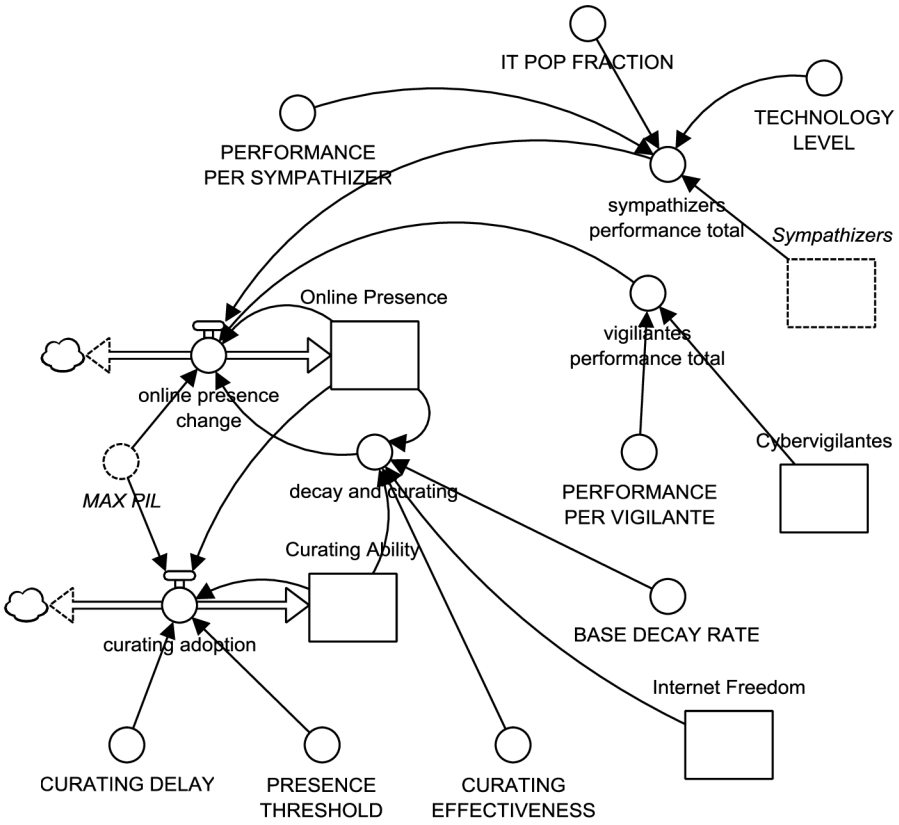
Rovnice 8 – změna dopadu džihádismu na veřejnost

Výstup z tohoto toku lze opět ukázat na pár příkladech. Následují tři grafy (č. 15), na prvním z nich je průběh produkovaný historickou posloupností obětí teroristických útoků a další dva zobrazují simulované chování endogenně generované modelem. I zde lze pozorovat častou podobnost mezi historickým a simulovaným chováním a zároveň sledovat občasné zásadní výkyvy, které se silně odchylují od historického chování za zkoumané desetileté období.



Grafy 15 – grafy zobrazující modelovaný dopad na veřejnost produkovaný oběťmi teroristických útoků

7.2.6 Segment soupeření v kyberprostoru



Obrázek 27 – diagram stavů a toků segmentu modelu zachycujícího soupeření mezi stranami v kyberprostoru

Hlavním uzlem této poloviny modelu, která zachycuje děje v kyberprostoru a soupeření o jeho využívání k podpoře a šíření džihádismu, jsou tok a stav, ve kterém se sbíhá působení džihádistických sympatizantů, kybervigilantistů odporujících džihádismu a snahy správců digitálního obsahu o jeho regulaci či přímo cenzuru (obr. 27). Tento stav nazvaný *Online Presence* opět využívá škály od 0 do 1 a vyjadřuje rozšířenost džihádistické propagandy v kyberprostoru a dostupnost jejich materiálů (včetně návodů) na sociálních médiích, webových stránkách i fórech. Vysoká hodnota této proměnné značí vysokou relativní saturaci, snadnou dostupnost a vysokou pravděpodobnost, že člověk na tento typ obsahu narazí, aniž by jej explicitně vyhledával. Spadá sem také informační bezpečnost a zajištění anonymity autorů a šiřitelů džihádistického obsahu.

Síla, která navyšuje výskyt džihádistické propagandy a dalších materiálů, se v modelu přímo odvozuje od počtu sympatizantů této ideologie a koeficientů, které určují jejich kapability. Ty ve

skutečnosti pokrývají velice široké spektrum od lidí takřka IT-negramotných až po velmi kompetentní hackery,[67] nicméně v modelu je zapotřebí tuto komplexitu zredukovat až na jedinou souhrnnou proměnnou (*sympathizers performance total*). Toto zjednodušení mimo jiné vychází z postupující vertikální i horizontální proliferace informačních technologií a jejich rostoucí role ve společnosti (*TECHNOLOGY LEVEL* a *IT POP FRACTION*). Lze tedy očekávat, že i při teoretickém zachování počtu džihádistických sympatizantů by jejich schopnost působit v kyberprostoru a využívat jej k vlastním záměrům pomalu rostla.

Podobným způsobem působí i protidžihádističtí vigilantisté. Od první skupiny se ale odlišují mnohem nižšími celkovými počty a zároveň mnohem vyšší průměrnou úrovní schopností v kyberprostoru působit. Přestože tedy obě skupiny ve svých řadách mají hackery schopné způsobit vážné škody v počítačových sítích a informačních systémech svých cílů a zároveň obsahují i „pouhé“ šiřitele a přeposílače propagandy, jejich relativní poměr a koncentrace jsou v zásadě opačné. Od čeho a jak se odvíjí počet kybervigilantistů řeší až následující podkapitola.

Třetí silou je regulace a cenzura ze strany poskytovatelů a správců obsahu (často pod tlakem národních vlád, viz kapitola 3.4). Ti se zpožděním reagují na neakceptovatelnou úroveň výskytu nežádoucího (a někdy i ilegální) obsahu jeho odstraňováním, blokováním účtů atp. (*Curating Ability*). V modelu je k tomu přidán i běžný proces takzvaného digitálního tlení (*BASE DECAY RATE*), který reprezentuje samovolné zanikání, technické potíže, zapomínání a ztrátu zájmu o webové stránky a sociální účty.

```
online_presence_change
       = (sympathizers_performance_total
         - vigiliantes_performance_total
         - decay_and_curating)
         * (MAX_PIL - Online_Presence)/(MAX_PIL)



       = ((Sympathizers * IT_POP_FRACTION * TECHNOLOGY_LEVEL *
           PERFORMANCE_PER_SYMPATHIZER)
         - (Cybervigilantes * PERFORMANCE_PER_VIGILANTE)
```

[67] Za povšimnutí stojí případ britského hackera jménem Junaid Hussain, který byl nejprve pod jménem TriCk jednou z klíčových postav hacktivistické skupiny TeaMp0isoN (která navíc příležitostně spolupracovala s Anonymous) a později deklarovaným členem ISIS a jedním z hlavních hackerů tzv. *CyberCaliphate*. Pod jménem Abu Hussain al-Britani byl v roce 2015 zabit útokem bezpilotního letounu poblíž syrského města Rakka (viz Murphy 2015).

```
        - (BASE_DECAY_RATE * Online_Presence + Curating_Ability *
          CURATING_EFFECTIVENESS/Internet_Freedom))
        * (MAX_PIL - Online_Presence)/(MAX_PIL)
      = ((Sympathizers * 0.02 * (1+RAMP(0.1/52, 0)) * 2.5e-7)
        - (Cybervigilantes * 1e-5)
        - (4e-3 * Online_Presence + Curating_Ability * 2e-3/Internet_Freedom))
        * (1 - Online_Presence)/(1)
```

Rovnice 9 – změna výskytu džihádismu v kyberprostoru

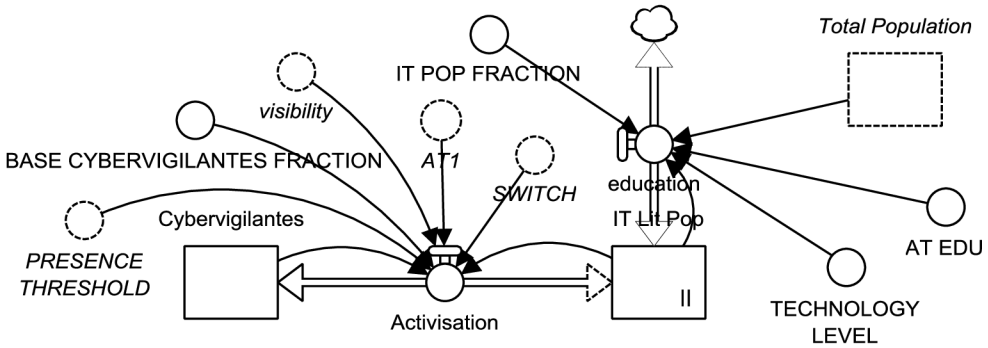
```
curating_adoption
      = ((MAX_PIL - Curating_Ability)^2/MAX_PIL^2)
        *SMTH3(Online_Presence - PRESENCE_THRESHOLD, CURATING_DELAY)
        /(CURATING_DELAY/10)
      = ((1 - Curating_Ability)^2/1^2)
        *SMTH3(Online_Presence - 0.2, 52)
        /(52/10)
```

Rovnice 10 – výpočet vývoje síly regulace digitálního obsahu

Růst obou stavů je opět nelineární a podobně jako v případě předchozí podkapitoly se rychlost jejich přítoků mění v závislosti na aktuální hladině. Zde je však situace o něco jednodušší a ke zpomalení dochází pouze s přibližováním se maximální hodnotě, nikoliv při hodnotách nízkých. Při konstantních vstupech je přítok tím rychlejší, čím blíže je stav nule, a postupně se zpomaluje s tím, jak se stav přibližuje hodnotě 1. Toto je zajištěno pronásobením vstupů rozdílem mezi maximální a aktuální hladinou stavu: *MAX PIL – Online Presence*. Tento činitel se blíží 0, když se stav blíží 1.

Pro fungování modelu to znamená, že navýšit výskyt propagandy a džihádistických materiálů v kyberprostoru je relativně snadné, dokud je tento výskyt relativně nízký. Jakmile dojde k tomu, že je v kyberprostoru této propagandy již relativně hodně, stává se jeho další navyšování podstatně obtížnější, neboť je už v zásadě nasycen. Podobně i zavádění prvních regulatorních opatření a filtrování obsahu bývá v zásadě přímočaré, neboť je z počátku poměrně snadné ohraničit neakceptovatelný obsah a příspěvky. Postupem času se ale tato hranice rozmělňuje a s rostoucí agresivitou cenzury je čím dál obtížnější cílový obsah jednoznačně definovat a zároveň zabránit tomu, aby došlo k antagonizaci legitimních uživatelů.

7.2.7 Vigilantistický segment



Obrázek 28 – diagram stavů a toků segmentu modelu zachycujícího vývoj a aktivizaci protidžihádistických vigilantistů v kyberprostoru

Předposlední z popisovaných segmentů modelu (obr. 28) řídí počet aktivní vigilantistů, kteří napadají, blokují a jinak narušují využívání kyberprostoru džihádisty a jejich sympatizanty. Tento segment do značné míry navazuje na úplně první z popisovaných segmentů, tedy ten demografický. Maximální možné množství kybervigilantistů, potažmo hacktivistů obecně, je omezeno celkovou populací a především tou její částí, která je dostatečně zdatná v informačních technologiích, aby se mohla podílet na kybernetických útocích (bez ohledu na jejich typ či motivaci). Z celkové populace je tak vydělena takto vzdělaná část (*IT Lit Pop*) a to bez ohledu na to, zda se jedná o formální vzdělání či samouky. Střední doba takového vzdělávání je v modelu nastavena na tři roky a podíl takto schopných lidí v modelu pomalu roste zároveň s již v předchozí podkapitole zmiňovanou neutuchající proliferací informačních technologií. Rovnice tohoto zobecněného a zjednodušeného vzdělávání vypadá takto:

```
education
      = (Total_Population*IT_POP_FRACTION*TECHNOLOGY_LEVEL-IT_Lit_Pop)/AT_EDU
      = (Total_Population*0.02*(1+RAMP(0.1/52, 0))-IT_Lit_Pop)/3*52
```

Rovnice 11 – tempo IT vzdělávání

Z této omezené populace se následně rekrutují lidé schopní a motivovaní bojovat proti džihádismu v kyberprostoru v podstatě bez ohledu na platné zákony, neboť to považují za potřebné (viz kapitola 3.3.2). Počet takto aktivizovaných vigilantistů se odvíjí od aktuální viditelnosti džihádismu ve společnosti, neboť o čím viditelnější problém se jedná, tím více z nich se rozhodne

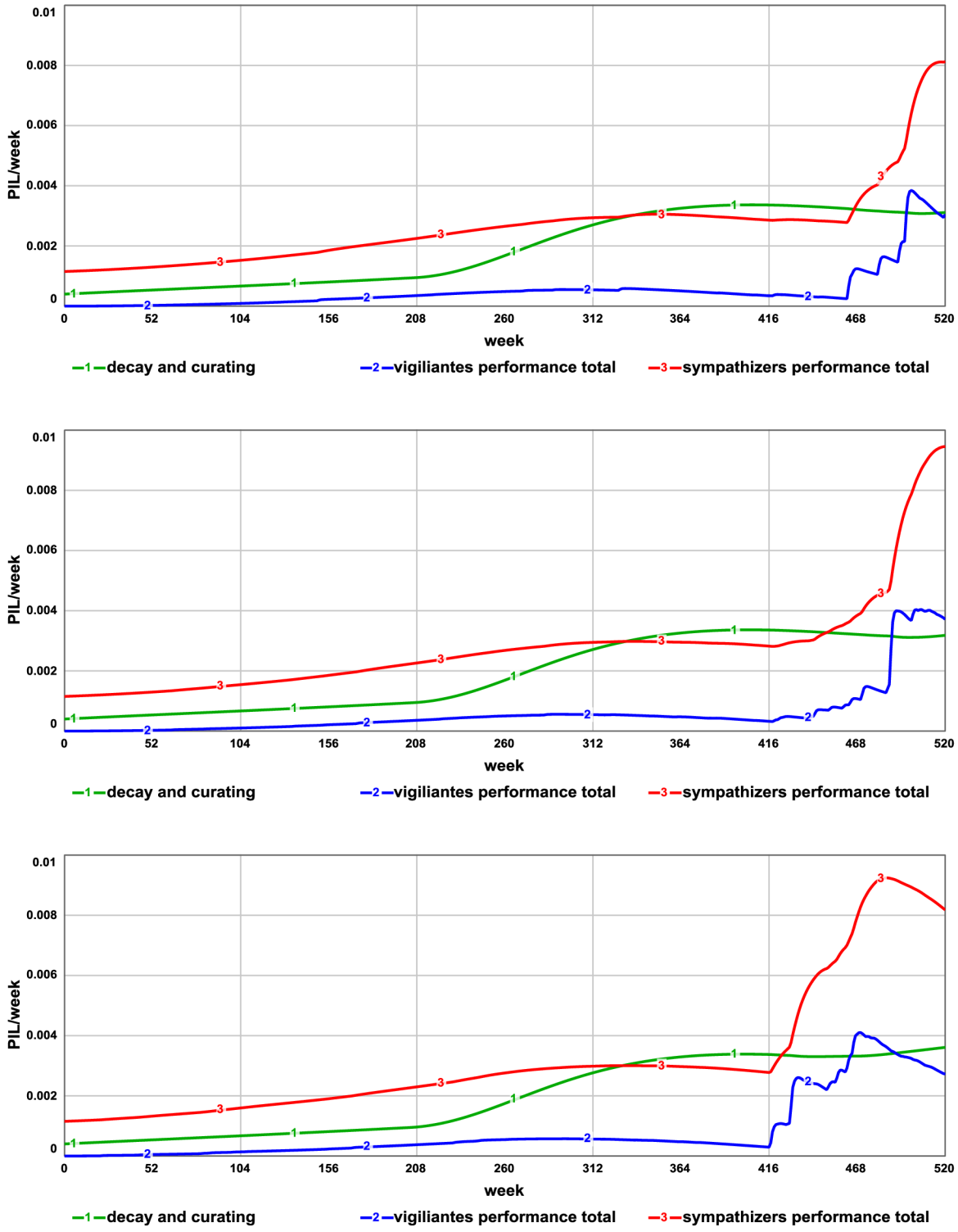
do konfliktu zapojit. V rovnici se rovněž nachází přepínač (*SWITCH*), který umožňuje snadno „vypnout kybervigilantismus“ a tak zkoušet simulovat model bez tohoto prvku a srovnat, jak se promění výsledné chování celého systému.

```
activisation
      = (IT_Lit_Pop * BASE_CYBERVIGILANTES_FRACTION
        * (IF SWITCH=2 THEN 0 ELSE 1)
        * MAX(0, (visibility - PRESENCE_THRESHOLD)) - Cybervigilantes)/AT1
      = (IT_Lit_Pop * 2e-5
        * (IF SWITCH=2 THEN 0 ELSE 1)
        * MAX(0, (visibility - 0.2)) - Cybervigilantes)/AT1
```

Rovnice 12 – tempo aktivizace protidžihádistických vigilantistů

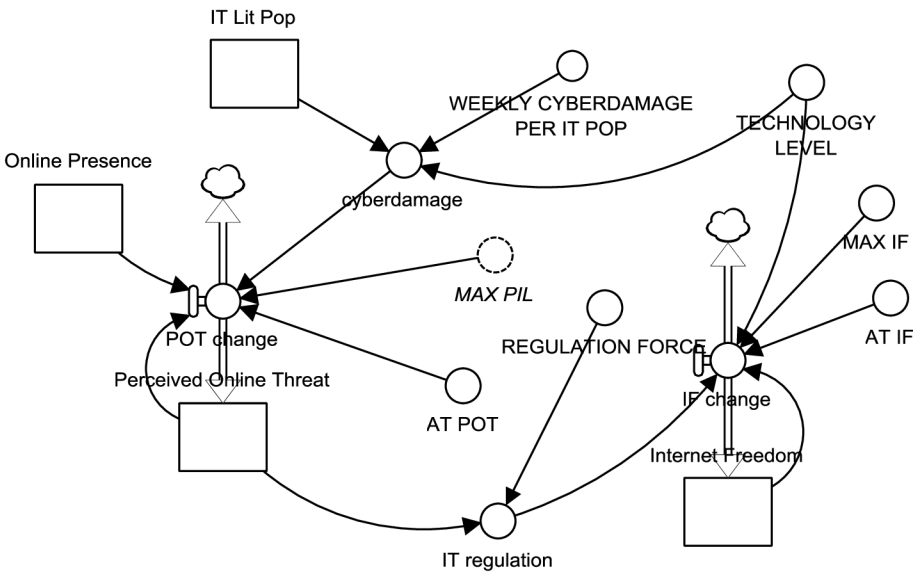
Tento proces probíhá velice rychle a zpětná vazba reaguje mnohem pružněji, než je tomu u poskytovatelů a zprostředkovatelů digitálního obsahu. Zároveň z toho však plyne i jejich o poznání kratší doba působení. Zatímco nově nastavená pravidla regulující nebo cenzurující obsah sociálních sítí a digitálních médií mohou mít působnost řadu let, vigilantisté mohou z nejrůznějších důvodů ztratit zájem dále se na tomto konfliktu podílet v řádu pouhých několika týdnů.

Na grafech č. 16 lze na třech ukázkách, z nichž ta první je opět produktem historických dat o obětech džihádistického terorismu na Západě za posledních deset let, sledovat vývoj všech tři modelovaných a popsaných vlivů na výskyt džihádismu online. Ze všech tří grafů je patrné, že dopad kybervigilantismu fluktuuje mnohem rychleji než jeho oficiální protějšek. Na pozorovaný vzestup džihádismu kybervigilantisté reagují téměř okamžitě eskalací vlastní aktivity, ale neudrží ji dlouhodobě, po prvotním vzepětí začne klesat a k dalšímu navýšení dojde jen v reakci na nové teroristické útoky. Vedle toho regulace a cenzura ze strany správců obsahu je daleko stabilnější, ale zase nestíhá reagovat na sledovaný prudký vzestup džihádismu.



Grafy 16 – grafy zobrazující modelované vlivy na výskyt džihádistické propagandy a příbuzných materiálů v kyberprostoru

7.2.8 Segment svobody a bezpečnosti v kyberprostoru



Obrázek 29 – diagram stavů a toků segmentu modelu zachycujícího vývoj a vnímání bezpečnosti a svobody v kyberprostoru

Poslední zachycený segment zkonstruovaného modelu je nepochybně tím nejvágnějším a tím, který se skládá z „nejměkčích“ proměnných. Základem jsou totiž dva stavy, které jsou jen těžko měřitelné, subjektivní a bez jednoznačných definic (natož jednotek). Svoboda a bezpečnost patří k odvěkým tématům a jejich současný význam, hodnota i role, kterou hrají a mají hrát v kyberprostoru, jsou stále předmětem aktivních debat (Serbu – Rotariu 2015, Schneier 2013, Ammori – Poellet 2010, Nojeim 2010, Dutta – Dutton – Law 2011).

Tato práce si v žádném případě neklade za cíl tuto věčnou debatu definitivně rozhodnout. Nepochybně je však zapotřebí blížeji specifikovat, co je v modelu těmito mlhavými názvy proměnných myšleno. Vnímaná hrozba (*Perceived Online Threat*) představuje to, do jaké míry je kyberprostor vnímán jako zdroj nebezpečí pro společnost a stát. K navýšení tohoto nevyhnutelně subjektivního dojmu přispívá vedle využívání internetu teroristy především kybernetická kriminalita, která je ve velmi zjednodušené podobě přítomna v modelu a na rozdíl od terorismu nebo hacktivismu je motivovaná spíše finančním ziskem. Finanční i společenské škody (v modelu jako *cyberdamage*) páchané tímto typem kriminality rovněž přirozeně rostou s pokračující proliferací informačních technologií, neboť kromě stoupajícího počtu možných pachatelů roste i množství a hodnota napadnutelných systémů (srov. Jardine 2015 a Europol 2016). Významný podíl na vnímání kyberprostoru jako bezpečnostní hrozby má také *Dark Web* (viz poznámka 15),

přirovnávaný k podsvětí internetu, kde kvete černý trh se zbraněmi, drogami, osobními údaji i dětskou pornografií i přesto, že čelí stálým snahám bezpečnostních složek o jeho infiltraci a likvidaci (Chertoff – Simon 2015, Greenberg 2017b, Leyden 2017).

Vedle toho svoboda (*Internet Freedom,* viz Kelly et al. 2016) je hodnotou, která vyjadřuje absenci regulací a dohledu v kyberprostoru, přičemž snahy o omezení této technologiemi poháněné svobody obvykle plynou z přesvědčení, že neregulovaný, anonymní a anarchický internet je bezpečnostní hrozbou. Právě v tomto bodě dochází na rčení, že k posilování bezpečnosti dochází na úkor svobody a soukromí. Rovnice obou toků i s rozvojem a dosazením konstant vypadají následovně:

```
POT_change
       = ((cyberdamage
         +Online_Presence)-Perceived_Online_Threat)
         *(MAX_PIL-Perceived_Online_Threat)/MAX_PIL/AT_POT
       = (((WEEKLY_CYBERDAMAGE_PER_IT_POP*IT_Lit_Pop*TECHNOLOGY_LEVEL)
         +Online_Presence)-Perceived_Online_Threat)
         *(MAX_PIL-Perceived_Online_Threat)/MAX_PIL/AT_POT
       = (((1e-10*IT_Lit_Pop*(1+RAMP(0.1/52, 0)))
         +Online_Presence)-Perceived_Online_Threat)
         *(1-Perceived_Online_Threat)/1/1
```

Rovnice 13 – změna vnímané hrozby v kyberprostoru

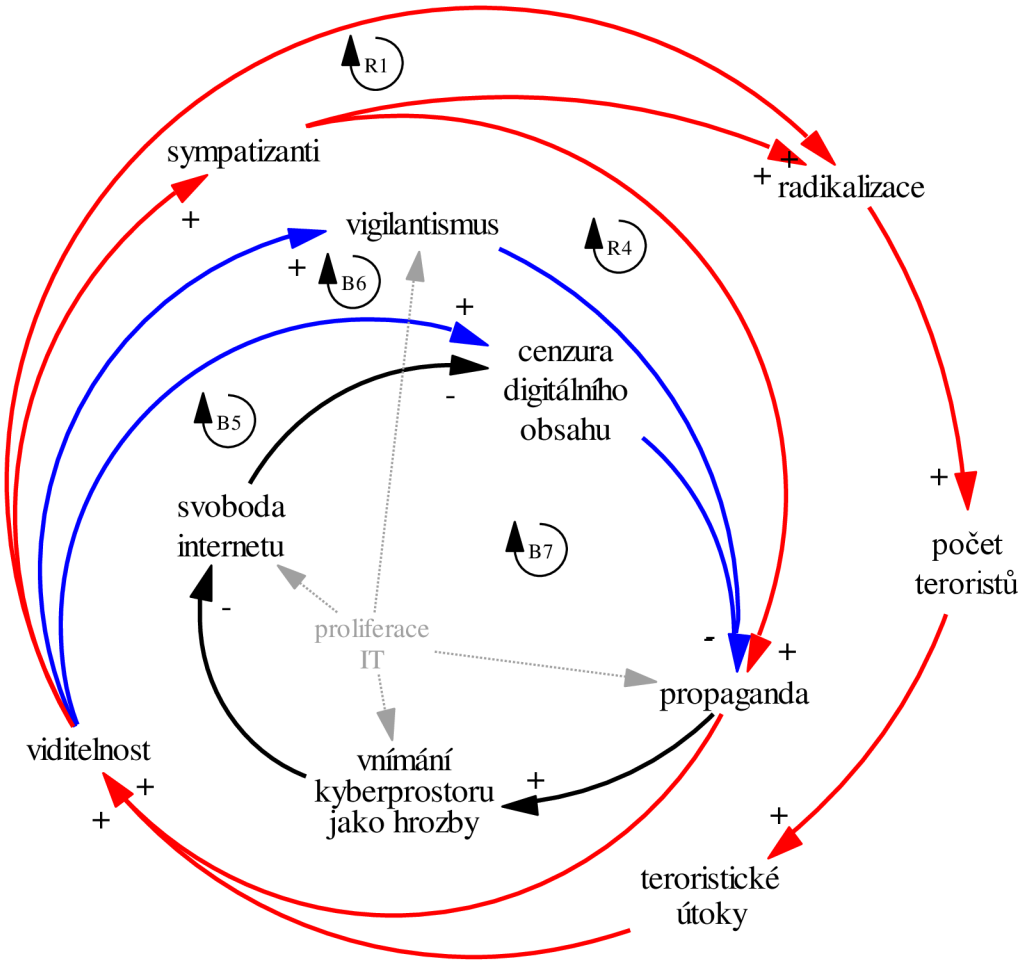
```
IF_change
       = ((MAX_IF - (IT_regulation
         /TECHNOLOGY_LEVEL)) - Internet_Freedom)
         *(Internet_Freedom*MAX_IF - Internet_Freedom^2)/(AT_IF*MAX_IF^2)
       = ((MAX_IF - ((Perceived_Online_Threat*REGULATION_FORCE)
         /TECHNOLOGY_LEVEL)) - Internet_Freedom)
         *(Internet_Freedom*MAX_IF - Internet_Freedom^2)/(AT_IF*MAX_IF^2)
       = ((1 - ((Perceived_Online_Threat*3)
         /(1+RAMP(0.1/52, 0)))) - Internet_Freedom)
         *(Internet_Freedom*1 - Internet_Freedom^2)/(52*1^2)
```

Rovnice 14 – změna vnímané svobody v kyberprostoru

Oba stavy opět užívají škály od 0 do 1 a rostou i klesají nelineárně, stejně jako tomu je u všech ostatních měkkých stavů, které jsou v modelu použity a aproximovány. Praktický dopad těchto zpětných vazeb na chování modelu je takový, že rostoucí výskyt džihádismu a rostoucí kyberkriminalita vedou ke zvýšenému vnímání kyberprostoru coby bezpečnostní hrozby, což se

projeví v pomalém poklesu svobody internetu, který nakonec pozitivně působí na efektivitu cenzury a regulace digitálního obsahu.

Na závěr rozboru struktury modelu je vhodné znovu ukázat smyčkový diagram, tentokrát ale se zdůrazněnými zpětnými vazbami z té poloviny modelu, která se zabývá kyberprostorem (obr. 30). V zájmu přehlednosti jsou vynechány zpětné vazby B2 a B3 (viz obr. 19) a namísto nich přibývá vyrovnávací zpětná vazba B7, která znázorňuje právě tento poslední segment. Zároveň je v diagramu vyznačena centrální role pokroku v informačních a komunikačních technologií, který žene kupředu hned několik prvků systému.



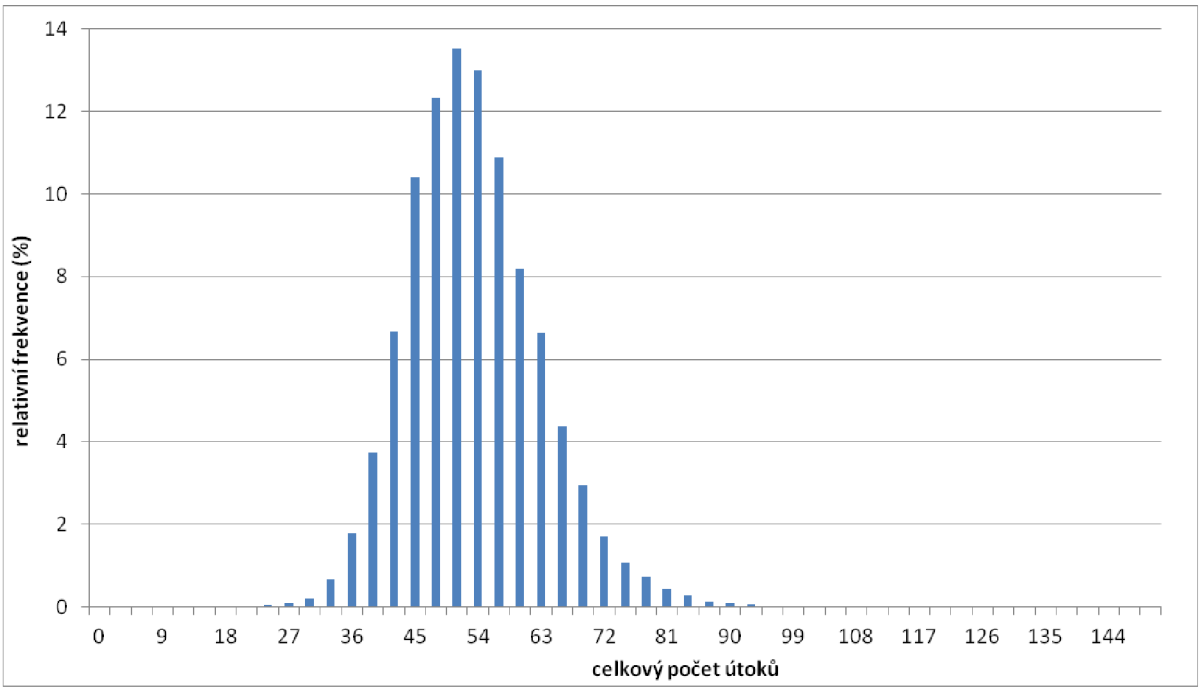
Obrázek 30 – diagram kauzálních smyček zaměřený na děje v kyberprostoru

7.3 Výsledky simulací

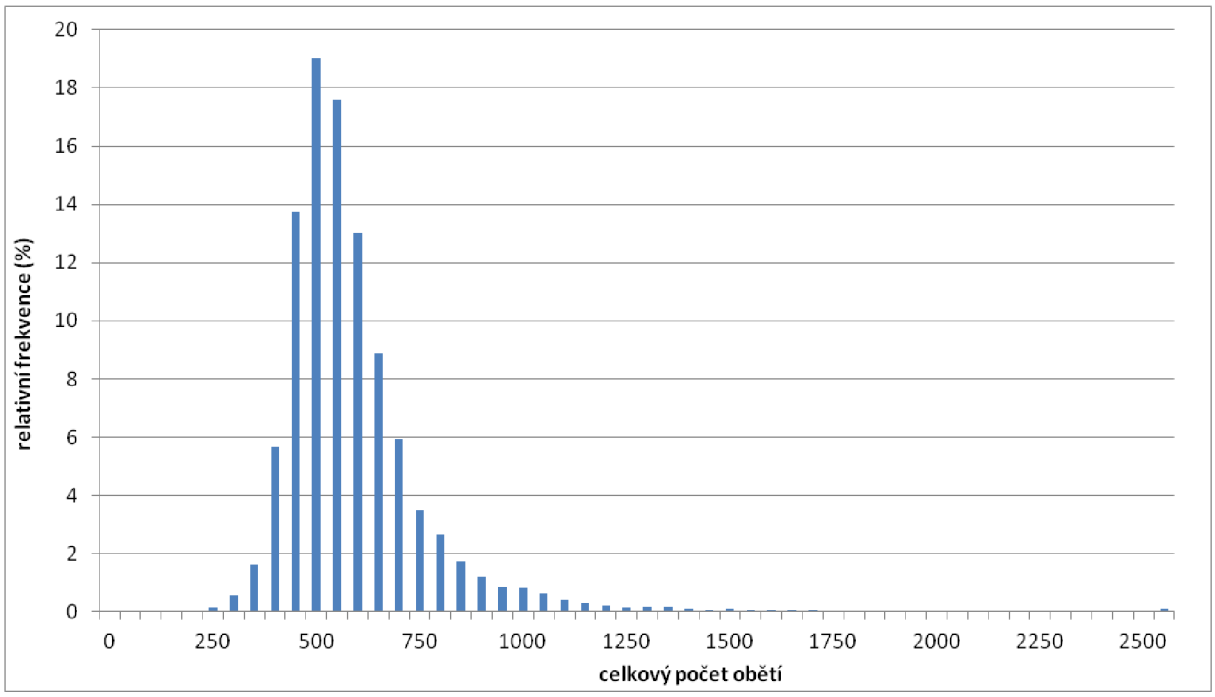
7.3.1 Replikace historie

Jak bylo popsáno výše (kapitola 4.3), individuální simulace mají kvůli své stochastické povaze takřka zanedbatelnou analytickou hodnotu a mohou sloužit pouze jako ilustrativní příklady konkrétního chování. Pro znázornění chování celého systému je proto nutné analyzovat celé série simulací, v tomto případě čítající deset tisíc opakování. Takto velký vzorek již je možné statisticky analyzovat a série vzájemně porovnávat.

Prvním milníkem, který model musí splňovat, je replikace historického chování a parametrů referenčního vzorku. Pro základní srovnání byly jako kontrolní body zvoleny celkový počet útoků a celkový počet obětí za desetileté sledované období. Z dat prezentovaných v šesté kapitole vyplývají tyto hodnoty jako 52 a 523. Model by se tak ve svém základním nastavení měl co nejvíce přiblížit těmto dvěma hodnotám, přičemž ve druhé kapitole byla akceptovatelná tolerance stanovena jako ± 5%, tj. 49.4 až 54.6 teroristických útoků a 496.85 až 549.15 obětí. Tyto hodnoty budou srovnávány s mediánem sérií simulací, neboť aritmetický průměr by byl příliš silně ovlivněn extrémními hodnotami na dlouhém chvostu generovaném mocninným zákonem.



Graf 17 - histogram relativních frekvencí počtů útoků během simulací v základním nastavení modelu



Graf 18 – histogram relativních frekvencí počtů obětí během simulací v základním nastavení modelu

Pro grafické znázornění výsledků celé série deseti tisíc simulací byly zvoleny histogramy (Graf 17 a Graf 18), které zobrazují frekvence daných konečných hodnot. Výška sloupců (svislá osa) ukazuje relativní četnost výskytu simulací, jejichž konečným výsledkem byl příslušný interval počtu obětí nebo teroristických útoků (vodorovná osa).

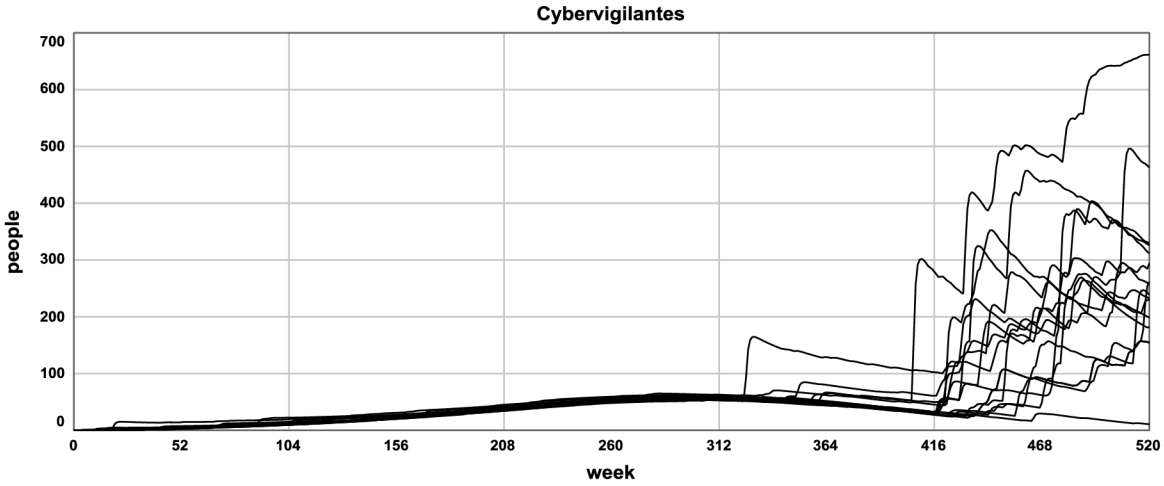
Již z histogramů je vidět, že frekvence je nejvyšší (téměř 14%, respektive 20%) v hodnotách blízkých těm historickým. Pro vyšší přesnost je ale třeba přejít k vypočítaným hodnotám pro tuto sérii:

	počet útoků	počet obětí
medián	**52.0**	**523.9**
průměr	52.4	568.6
směrodatná odchylka	9.5	266.9
maximum	133.0	16395.0
minimum	22.0	145.6

Tabulka 3 – statistické hodnoty pro sérii simulací v základním nastavení modelu

V konečném srovnání se medián simulací odchyluje od historických hodnot o méně než 1% v obou zvolených metrikách a to i přesto, že zahrnuje zcela extrémní běhy, které vygenerovaly více než dvouapůlnásobný počet teroristických útoků nebo dokonce třicetinásobný počet jejich obětí, přičemž se kupodivu nejedná o tentýž případ. V zobrazeném histogramu jsou tyto nejextrémnější hodnoty (nad 2500 obětí) shrnuty do malého červeného sloupce na pravém okraji a zde konkrétně představují 11 případů (0.11%). Vedle toho asi 3.5% simulací vedlo k více než dvojnásobku obětí oproti historickému průběhu.

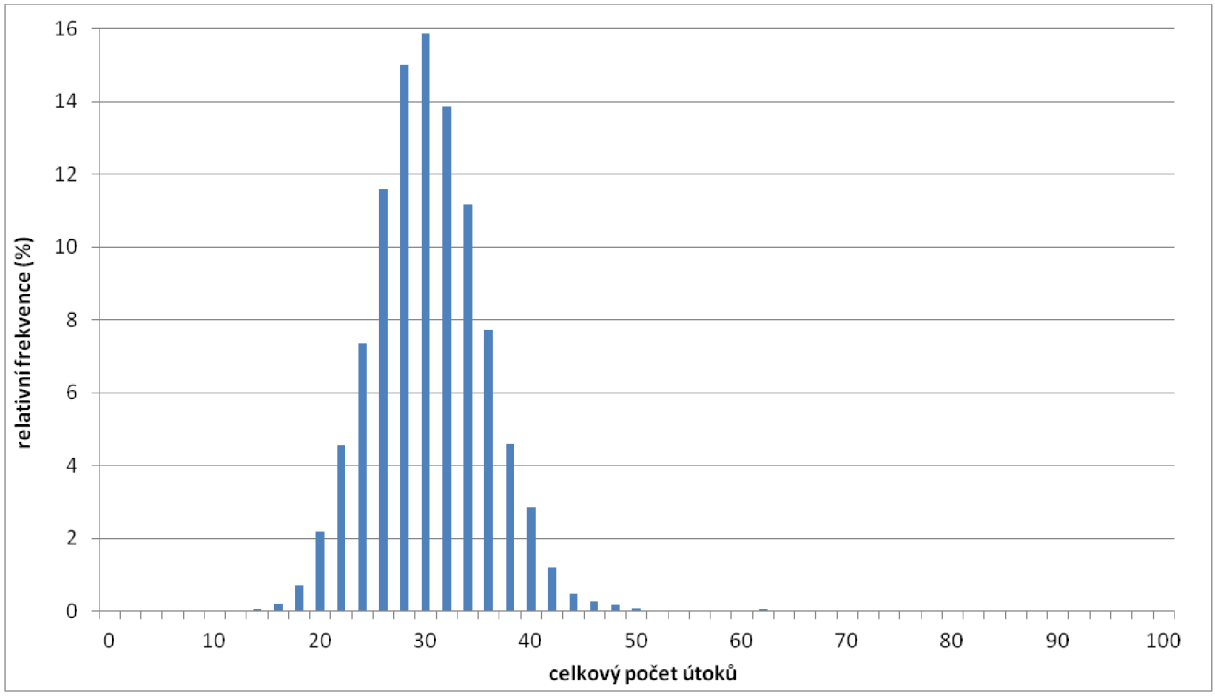
Jak se simulace postupně rozcházejí a dochází k jejich štěpení na více či méně odlišné scénáře lze ilustrovat na vývoji počtu modelem simulovaných vigilantistů bojujících proti džihádismu v kyberprostoru. Z grafu (Graf 19), na kterém je zobrazen počet těchto kybervigilantistů v průběhu patnácti náhodně vybraných simulací, je vidět, že k hlavnímu dělení dochází až kolem 416tého týdne, tedy na přelomu mezi osmým a devátým rokem běžících simulací, kdy do modelu exogenně vstupují „řízení“ teroristé, tedy ti, kteří typicky provádějí rozsáhlejší útoky s větším množstvím obětí a větší odezvou napříč celým modelovaným systémem. Během prvních osmi let lze sledovat relativně homogenní průběh napříč simulacemi, i když je ale patrné, že k výkyvům někdy dochází i před zmíněným zlomovým okamžikem a to v závislosti na generovaných teroristických útocích. Každopádně ale za tímto bodem lze již jen velmi těžko hledat nějaký společný nebo typický průběh, neboť kumulující se zpětné vazby ženou systém do různých směrů.



Graf 19 – komparativní graf počtu kybervigilantistů během patnácti simulací modelu v jeho základním nastavení

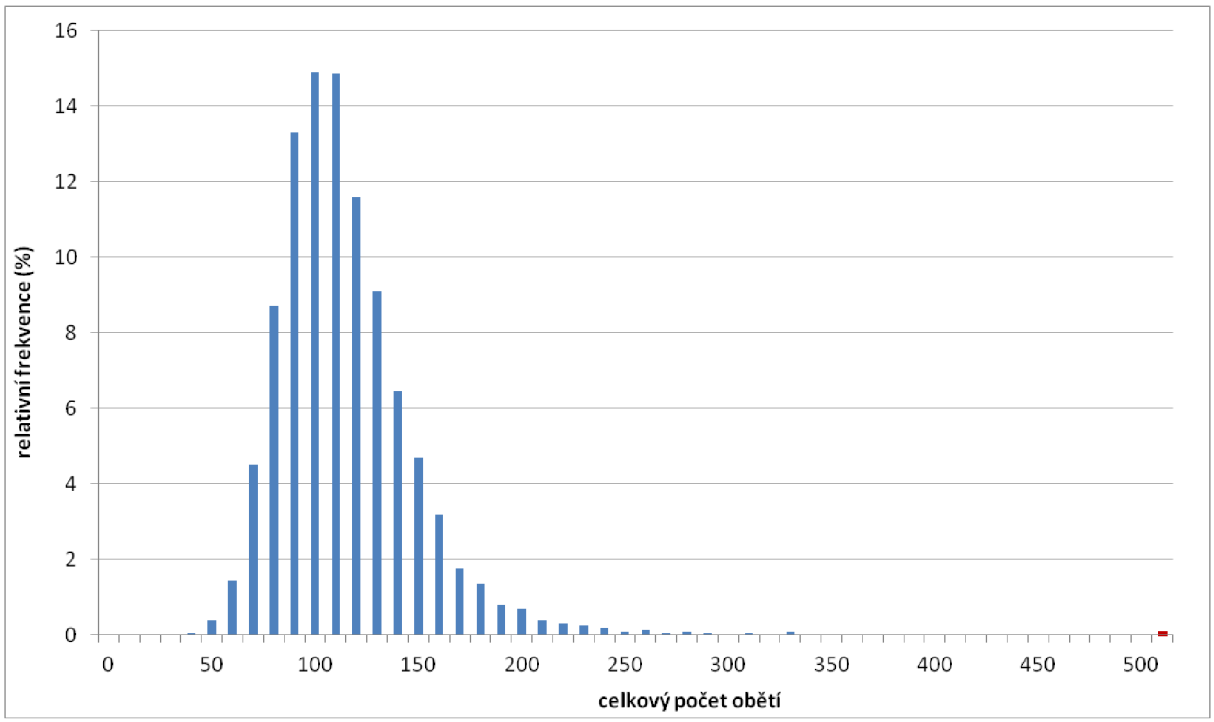
7.3.2 Bez eskalace řízeného terorismu

Druhým párem hodnot, na nichž lze testovat validitu modelu, je hypotetický scénář, u kterého nedochází ke vstupu řízených teroristů na přelomu let 2014 a 2015. Cílových hodnot, kterým by se model v tomto nastavení měl opět co nejvíce přiblížit, se lze dobrat jednoduchou extrapolací průběhu prvních osmi let. Z dat v referenčním vzorku vychází, že během prvních osmi let došlo k 23 útokům o 83 obětech, tedy průměrně ke 2.875 útokům ročně, které způsobily 10.375 obětí. Z toho vyplývají extrapolované desetileté sumy na 28.75 útoků a 103.75 obětí. Při užití stejné tolerance ± 5% jsou výsledné intervaly 27.3125 až 30.1875 pro počet teroristických útoků a 98.5625 až 108.9375 pro počet obětí.



Graf 20 - histogram relativních frekvencí počtů útoků během simulací bez eskalace

Po provedení deseti tisíc simulací, u nichž nedošlo k žádné exogenní eskalaci, jsou výsledné mediány 30 pro počet teroristických útoků a 104.4 pro počet jejich obětí (viz tabulka 2). Lze tedy konstatovat, že i v tomto režimu se podařilo reprodukovat cílové chování extrapolovaného systému, neboť odchylka činí jen asi 3% pro útoky a 1% pro oběti, a že model tímto obstál v obou dvou klíčových testech validity.



Graf 21 - histogram relativních frekvencí počtů obětí během simulací bez eskalace

	počet útoků	počet obětí
medián	**30.0**	**104.4**
průměr	29.7	111.0
směrodatná odchylka	5.3	45.0
maximum	74.0	1694.5
minimum	10.0	35.2

Tabulka 4 - statistické hodnoty pro sérii simulací bez eskalace

Přestože i zde lze nalézt extrémní případy, které medián mnohonásobně převyšují, toto nastavení modelu se svými výsledky zásadně odlišuje od základní verze a takřka mezi nimi neexistuje žádný překryv. Pouze 0.12% simulací bez exogenní eskalace překonalo hranici 500 celkových obětí a zároveň jen jedna jediná simulace v základním nastavení klesla pod 150 obětí. Pravděpodobnost, že by tyto dvě verze systémového modelu vyprodukovaly navzájem zaměnitelné výstupy, je tak opravdu velmi nízká, ba až zanedbatelná. K největšímu překryvu obou sérií simulací dochází v zóně kolem 300 obětí, ke kterým obě verze modelu směřují ve zhruba 0.25% případů.

Je až pozoruhodné, jak velký vliv může mít na ten samý systém jednorázový impuls ve formě malého počtu dobře organizovaných aktérů. Veškeré ostatní parametry obou verzí modelu jsou zcela totožné, a přesto produkují natolik odlišné výsledné chování. Přitom rozhodně neplatí, že by bylo možné celý rozdíl v počtech teroristických útoků a jejich obětí dát za vinu přidaným řízeným teroristům. I v základním nastavení totiž průměrně způsobují jen asi 17% ze všech teroristických útoků a kolem 70% obětí.[68]

Dalším důsledkem tohoto impulsu je zvýšení viditelnosti a tím i atraktivity džihádismu, který pak vede ke zrychlení radikalizace, nárůstu propagandy v kyberprostoru i mimo něj a nakonec i k vyšším počtům inspirovaných teroristů. Ti jsou sice mnohem méně efektivní při provádění útoků a mají na svědomí poměrně menší počty obětí, ale dramaticky zvyšují počet útoků, ke kterým v systému dochází. To vede k udržování viditelnosti džihádismu a pokračující radikalizaci.

Podle těchto dvou sérií simulací to vypadá, že analyzovaný systém má tak jako tak potenciál k tomuto chování a je díky své vnitřní struktuře (tj. zejména posilujícím zpětným vazbám) vždy schopen produkovat chování vedoucí k vyšším počtům teroristických útoků a jejich obětí. Za normálních okolností (tedy prvních osm let) k tomu ale nedochází, neboť chybí dostatečně silný impuls, který by systém na tuto „kolej“ posunul. Může k tomu sice dojít i endogenně, tedy díky chaotické povaze terorismu, ale pravděpodobnost je velmi nízká. Od roku 2014 tento impuls poskytl především takzvaný Islámský stát a jím řízení teroristé (přímo či virtuálně), kteří na území Západu spustili iniciační vlnu teroristických útoků, čímž došlo i k nárůstu džihádismem pouze inspirovaných útoků.

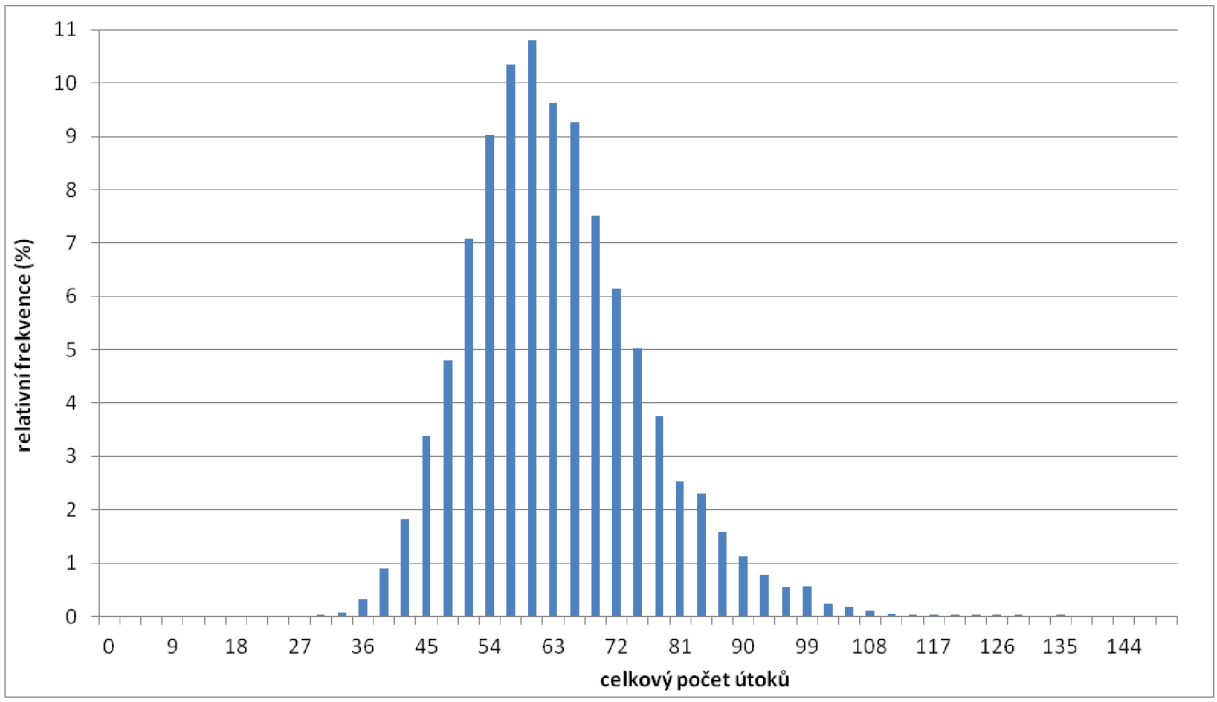
Analogicky lze tuto situaci připodobnit třeba k balónu, který se nachází v terénu profilem se podobající sopce. Je-li balón nahoře v „kráteru“, běžné děje (například vítr) jej jen těžko vynesou přes jeho okraj. Každá menší síla jej sice vychýlí z klidové pozice a posune nahoru směrem k okraji, ale gravitace či tření jej vždy zbrzdí a nakonec i vrátí zpět doprostřed. Pravděpodobnost, že by se balón samovolně dostal mimo kráter, je velmi nízká. Pokud mu je ale dodán dostatečně silný impuls (třeba tím, že do něj někdo kopne), může doletět nebo se dokutálet až k okraji kráteru a přejít přes něj. Díky tomu se začne balón kutálet dolů a sám nabírat rychlost, dokud se nakonec nezastaví v nějakém nižším údolí.

---

[68] Není náhodou, že se tyto hodnoty velice přibližují k Paretovu pravidlu (viz kapitola 4.3) a jeho poměru 80:20. Zde jej tedy lze interpretovat tak, že asi k 80% obětí dojde během 20% teroristických útoků.

7.3.3 Bez vigilantismu v kyberprostoru

Aby bylo možné odpovědět na otázku, jak velký vliv má na chod celého systému protidžihádistický vigilantismus v kyberprostoru, je třeba provést další sérii deseti tisíc simulací, ovšem tentokrát bude namísto řízeného terorismu odstraněn vliv vigilantismu. Pro tuto sérii již neexistuje žádný interval, podle kterého by model bylo možné posuzovat, neboť se jedná o zcela spekulativní scénář, jehož účelem je pouze odhalit a odhadnout sílu vlivu konkrétního prvku systému, respektive proměnné modelu.

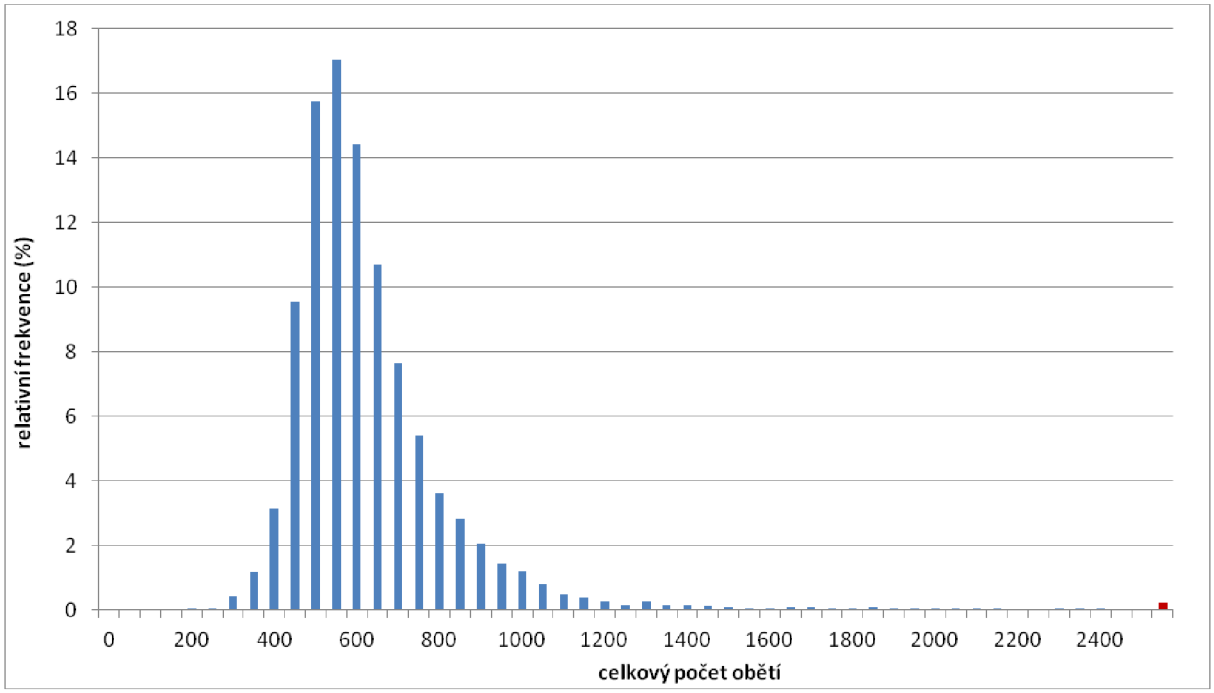


Graf 22 - histogram relativních frekvencí počtů útoků během simulací bez kybervigilantismu

V obou sledovaných hodnotách lze po odebrání kybervigilantismu z modelu (konkrétně pomocí zafixování počtu vigilantistů samotných na 0) sledovat jejich nárůst. V obou případech se ale jedná o nárůst poměrně nízký, což platí obzvláště v případě celkového počtu obětí teroristických útoků, jejichž medián narostl o necelých 7% z 524 na 560. Nebýt tak velkého použitého vzorku, bylo by vzhledem ke stochastické povaze modelu možné tento rozdíl zavrhnout jako chybu měření plynoucí z jeho pseudonáhodných prvků. Ovšem díky obrovskému počtu opakovaných simulací je tento rozdíl možné považovat za konzistentní a replikovatelný.

V počtu útoků lze pozorovat o něco větší nárůst a to zhruba 18%. Tento nesoulad mezi oběma nárůsty plyne z toho, že kybervigilantismus tak, jak je implementován v modelu, brzdí pouze inspirované útoky, které jsou typické relativně vysokou frekvencí a zároveň nízkým počtem obětí. Odebráním vigilantismu tak v modelu dojde k navýšení počtu inspirovaných útoků, ale ty mají obvykle na svědomí jen malé množství obětí, tudíž navýšení této hodnoty je v porovnání s první hodnotou znatelně menší.

V porovnání se základním režimem došlo navíc i ke zvýšení nejistoty a variability chování v modelu, a nikoliv jen k prostému posunutí histogramu doprava. Směrodatná odchylka vzrostla o 13% a počet extrémních případů nad 2500 obětí se více než zdvojnásobil.

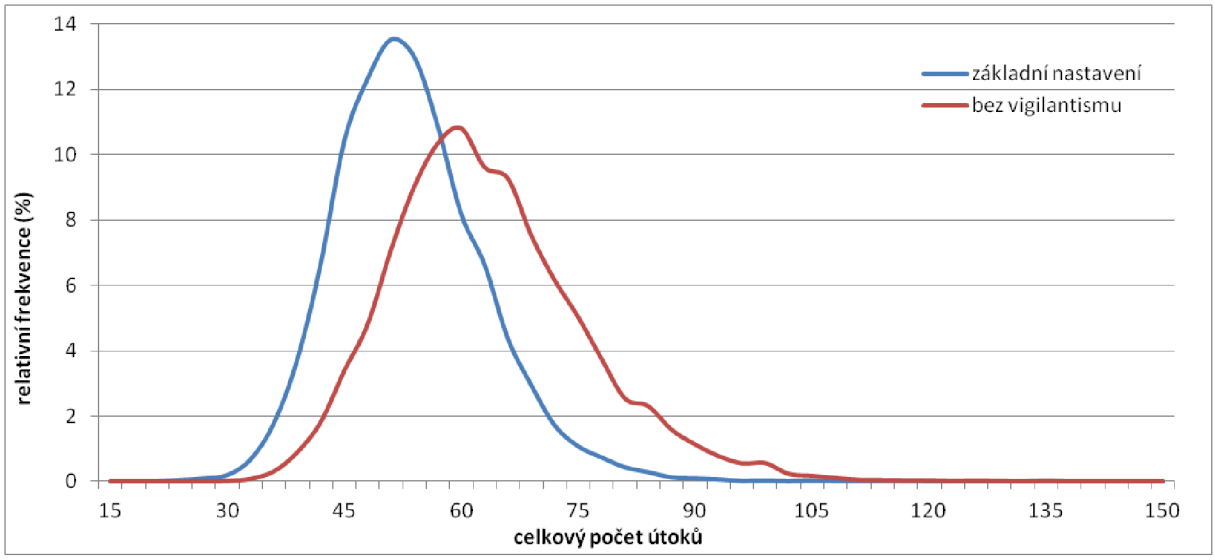


Graf 23 - histogram relativních frekvencí počtů obětí během simulací bez kybervigilantismu

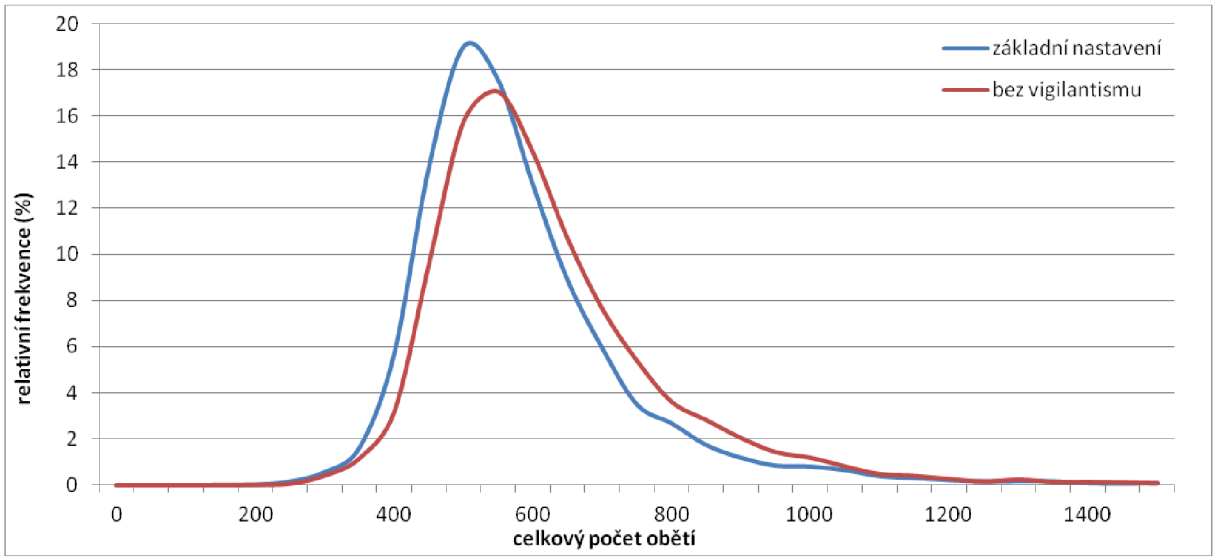
	počet útoků	počet obětí
medián	**61.0**	**559.5**
průměr	62.3	608.8
směrodatná odchylka	12.4	302.3
maximum	135.0	18988.4
minimum	30.0	187.2

Tabulka 5 - statistické hodnoty pro sérii simulací bez kybervigilantismu

Vymění-li se v histogramu sloupce za vyhlazené křivky, je možné výsledky obou dvou sérií i přehledně vizuálně srovnat. Na obou grafech je pak názorně vidět to, co již vyplývalo z naměřených hodnot, tedy že po vyřazení vlivu protidžihádistického kybervigilantismu došlo k mírnému posunu obou mediánů k vyšším hodnotám a zároveň i ke korespondujícímu zvýšení jejich odchylek. To je patrné z nižších a zároveň širších grafů pro série simulací bez vigilantismu, neboť plochy pod křivkami musí být zcela stejné (je-li pominuto mírné zkreslení způsobené jejich grafickým vyhlazením).



Graf 24 – srovnání histogramů počtů útoků mezi modely včetně a bez kybervigilantismu

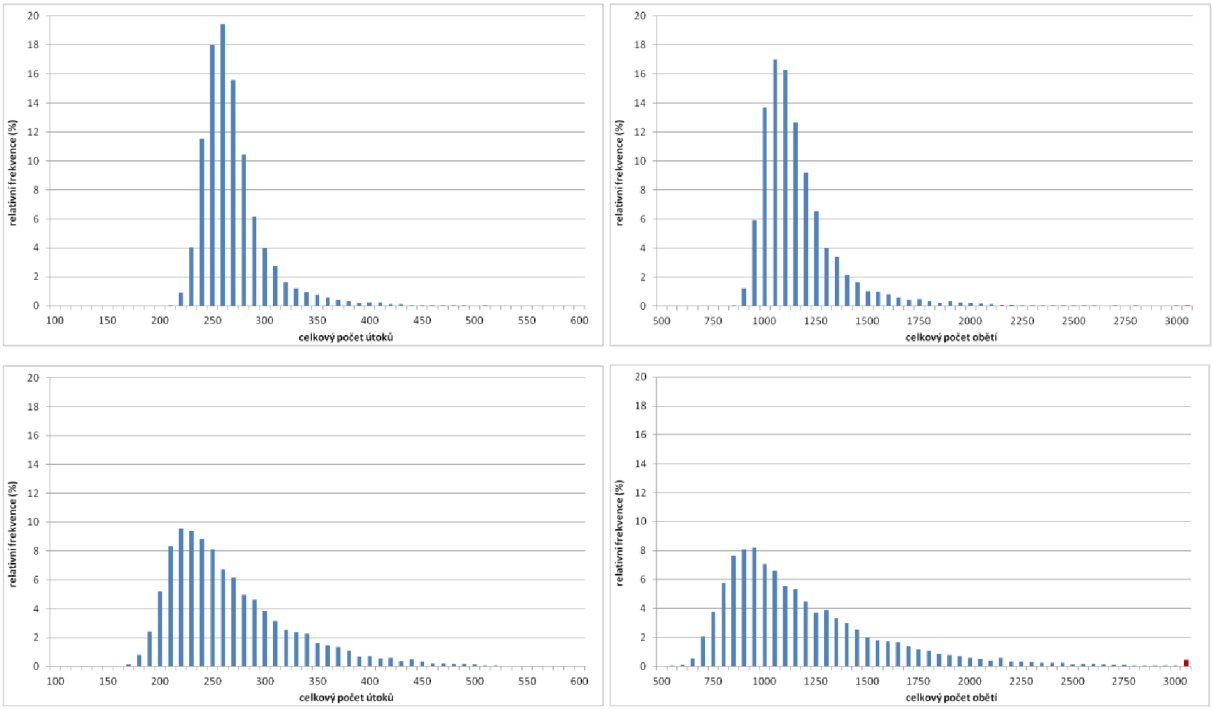


Graf 25 - srovnání histogramů počtů obětí mezi modely včetně a bez kybervigilantismu

7.3.4 Navázání na historický vývoj

Dynamický model systému umožňuje vedle replikování historie a manipulace s proměnnými také protažení simulací do budoucna. Implicitním předpokladem samozřejmě je, že základní struktura systému zůstane po celou dobu zachována a ani nedojde k žádným nepředvídaným a nepředvídatelným vnějším zásahům, které by významně ovlivnily jeho výsledné chování. Vzhledem k tomu, že tento konkrétní systém je silně závislý na volatilních sociálních i politických dějích a zároveň na neutuchajícím vývoji relevantních technologií (který navíc všeobecně akceleruje), je takovýto předpoklad poměrně naivní. I přesto může být takový výhled do budoucna přínosný při úvahách o směřování systému nebo o možnosti ovlivnění jeho chodu, ale přitom je nezbytně nutné mít na paměti jeho omezení, obzvláště v kontextu komplexních sociálních systémů.

Existují ale dvě možnosti, jakým způsobem pojmout pokračování simulace v základním režimu. Vedle přímočarého protažení simulace o dalších 520 týdnů lze totiž navázat na historický vývoj a prvních deset simulovaných let nahradit daty z referenčního vzorku. Vznikne tak projekce modelu do budoucna, která je o poznání více ukotvená v současném stavu a přímo z něj vychází.

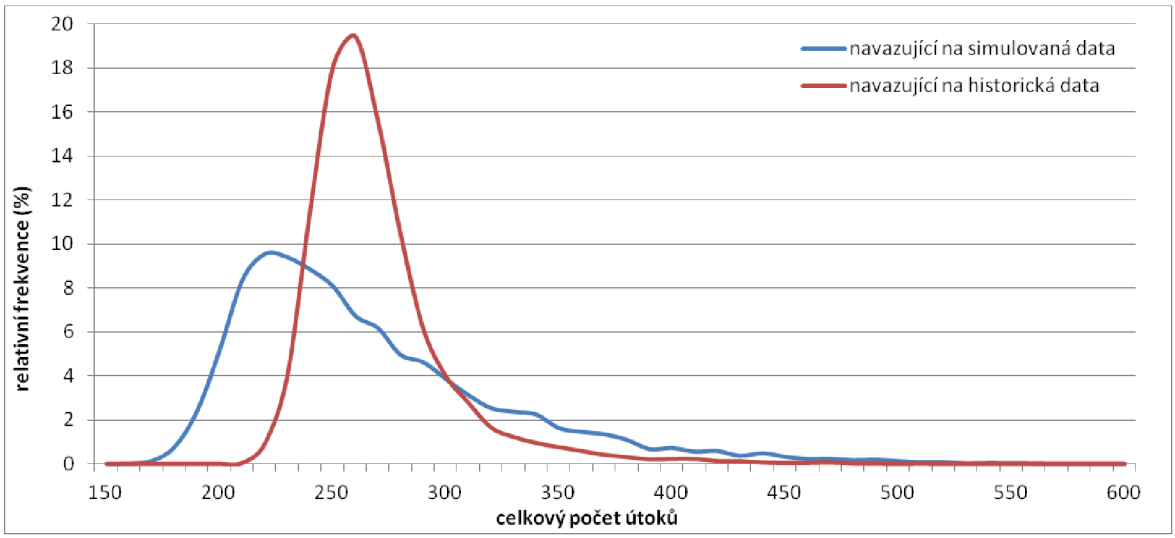


Grafy 26 – histogramy sérií prodloužených simulací, nahoře navazující na historická data, dole simulované na celých 20 let

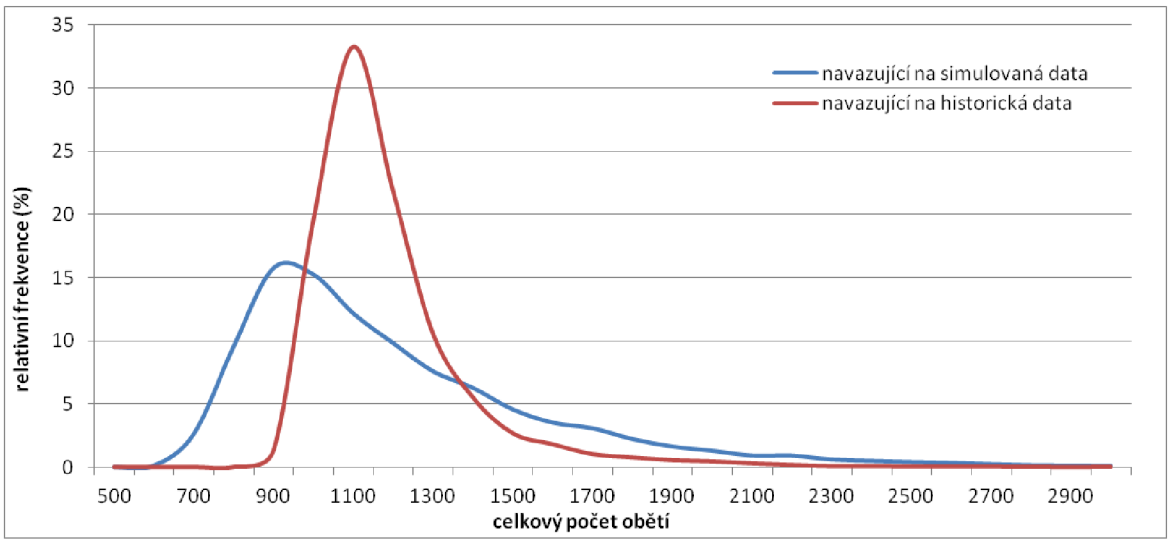
počet útoků	počet obětí

návaznost série:	historická	simulovaná	historická	simulovaná
medián	**258.0**	**247.0**	**1086.0**	**1051.5**
průměr	264.4	261.9	1135.1	1176.6
směrodatná odchylka	30.9	59.4	200.9	843.2
maximum	507.0	559.0	5058.3	69150.3
minimum	207.0	160.0	841.9	547.9

Tabulka 6 – srovnání statistických hodnot mezi sériemi prodloužených simulací navazujících na historická a simulovaná data



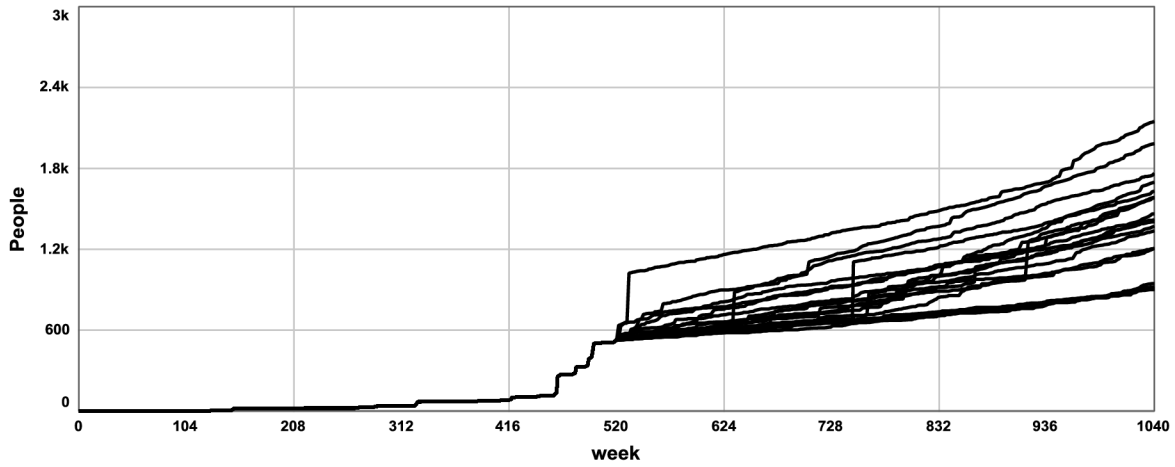
Graf 27 - komparace histogramů počtů útoků u prodloužených simulací



Graf 28 – komparace histogramů počtů obětí u prodloužených simulací

Z tabulky i všech histogramů je vidět velká podobnost mediánů obou sérií simulací modelu (rozdíl je v nízkých jednotkách procent) a zároveň očekávaný několikanásobný rozdíl ve směrodatné odchylce a variabilitě. Bez ohledu na to, zda simulace navazuje na historická data nebo pouze na simulovaný průběh prvních deseti let, celkové směřování modelu zůstává stejné. Distribuce výsledků simulací, které navazují na historii, je ovšem podstatně užší, neboť spektrum možností je zúženo již předem zafixovaným vývojem během prvních deseti let. Model má tak méně prostoru vybočit svým chováním dále od středu, který se nalézá v okolí 1070 obětí.

Až pozoruhodně rozdílná jsou u obou sérií simulací jejich maxima. Maximální naměřený celkový počet obětí prodloužených simulací navazujících na historická data je „pouhých“ 5058, přičemž maximum těch navazujících na simulovaný začátek je až neuvěřitelných 69150, tedy téměř čtrnáctkrát více. Přestože by mohlo být zajímavé pustit se do úvah o tom, jak by takový scénář mohl v realitě vypadat a co by se muselo přihodit, aby došlo k takovému množství obětí teroristických útoků, zde jsou prozaickou příčinou propojené zpětné vazby interagující s funkcemi s pseudonáhodnými prvky, které se v jedné z mnoha tisíc simulací zrovna sešly tak, že vygenerovaly takto extrémní výstup.

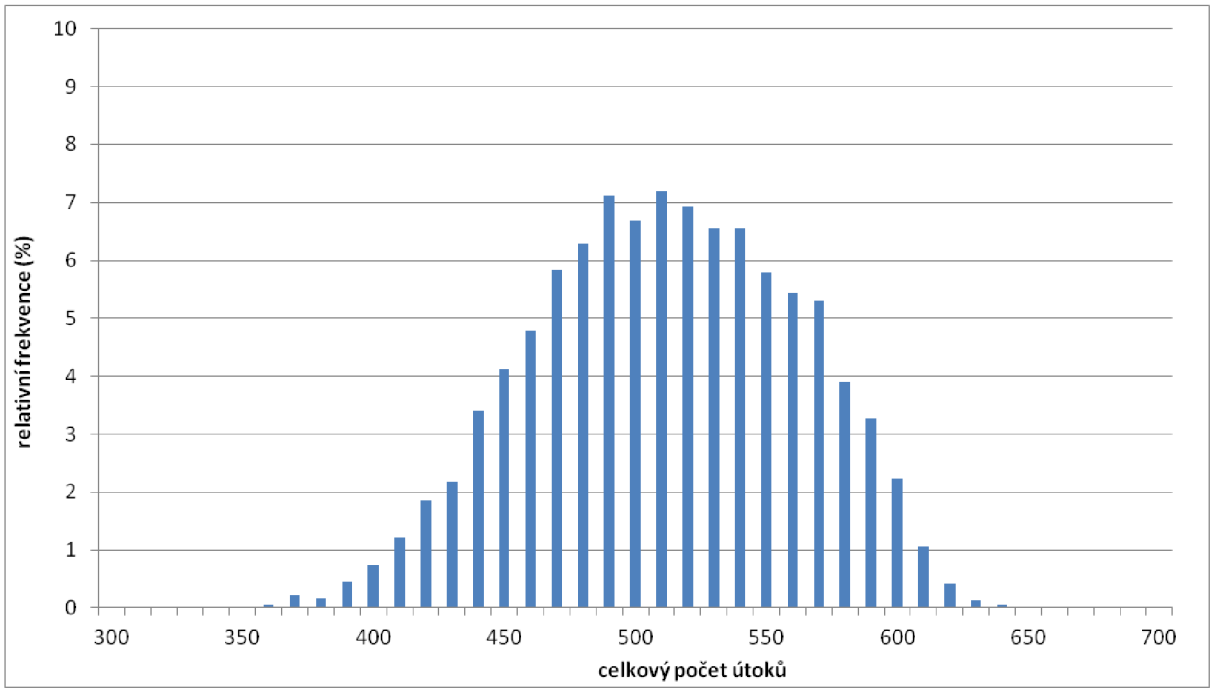


Graf 29 - komparativní graf celkových počtů obětí džihádistického terorismu během dvaceti prodloužených simulací modelu navazujících na historická data

Pro ilustraci je přiložen graf 29, který zachycuje vybrané spektrum simulací, které vycházejí ze situace na konci roku 2016. Jednotlivé linie znázorňují kumulující se oběti džihádistického terorismu na Západě, přičemž je patrné, že se začínají velmi rychle větvit ihned po dobrání historických dat a následném přechodu na dynamicky simulované teroristické útoky.

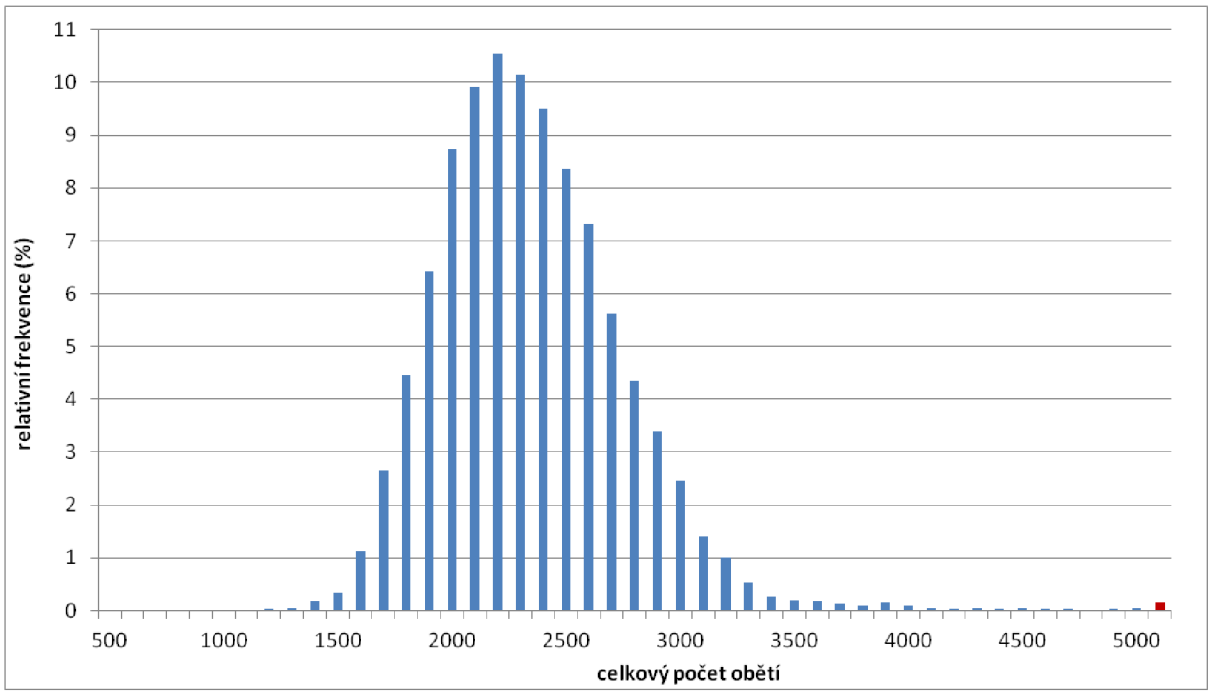
7.3.5 Extrapolace vlivu vigilantismu v kyberprostoru

Dále se přímo nabízí pokračovat v předchozím srovnání a protáhnout také grafickou i numerickou komparaci mezi základním modelem a modelem bez protidžihádistického kybervigilantismu o dalších deset let. V tomto případě se však ještě více stupňuje spekulativnost simulací, neboť vedle více či méně opodstatněného předpokladu, že během deseti let ve struktuře systému nedojde k žádné významné změně, hraje tu roli také fiktivní absence vigilantismu v systému.



Graf 30 - histogram relativních frekvencí počtů útoků během prodloužených simulací bez kybervigilantismu

Nepřítomnost vigilantismu a neschopnost systému včasně se adaptovat má na chování, které model vykazuje v dlouhodobějším horizontu, podstatně závažnější důsledky, než by se podle původních desetiletých simulací mohlo zdát. V tomto režimu je totiž zpětná vazba tlumící proliferaci džihádistické propagandy v kyberprostoru zcela nedostatečná ke zbrzdění prvotní eskalační vlny způsobené příchozími řízenými teroristy, a tak má tato zvýšená aktivita mnohem delší trvání, které se v původním desetiletém horizontu nestihá projevit. Navíc kvůli rostoucímu významu informačních technologií je toto zpoždění čím dál větším problémem.

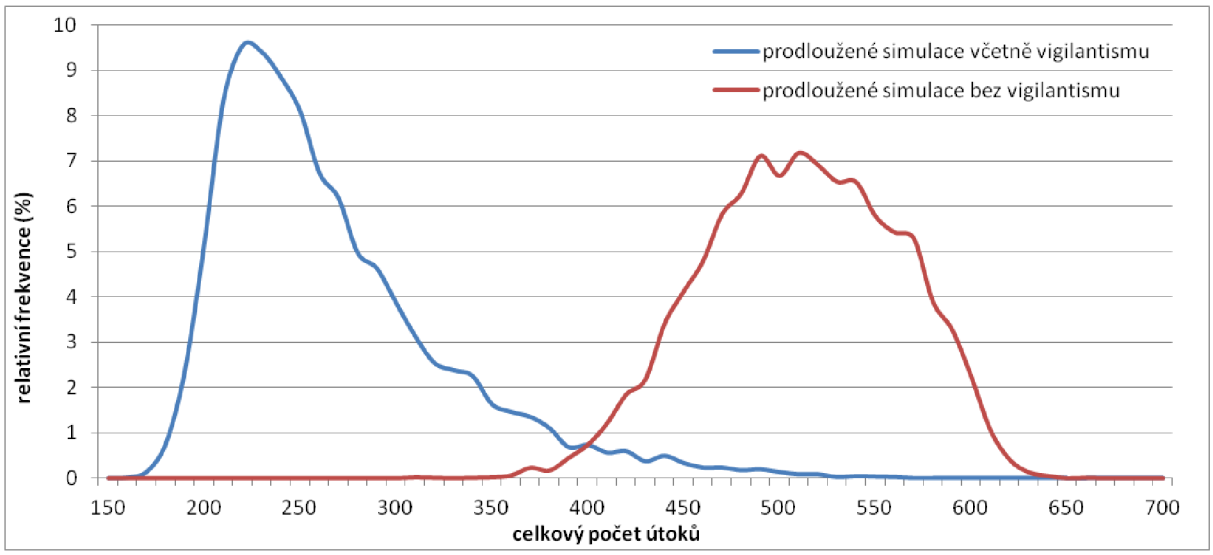


Graf 31 - histogram relativních frekvencí počtů obětí během prodloužených simulací bez kybervigilantismu

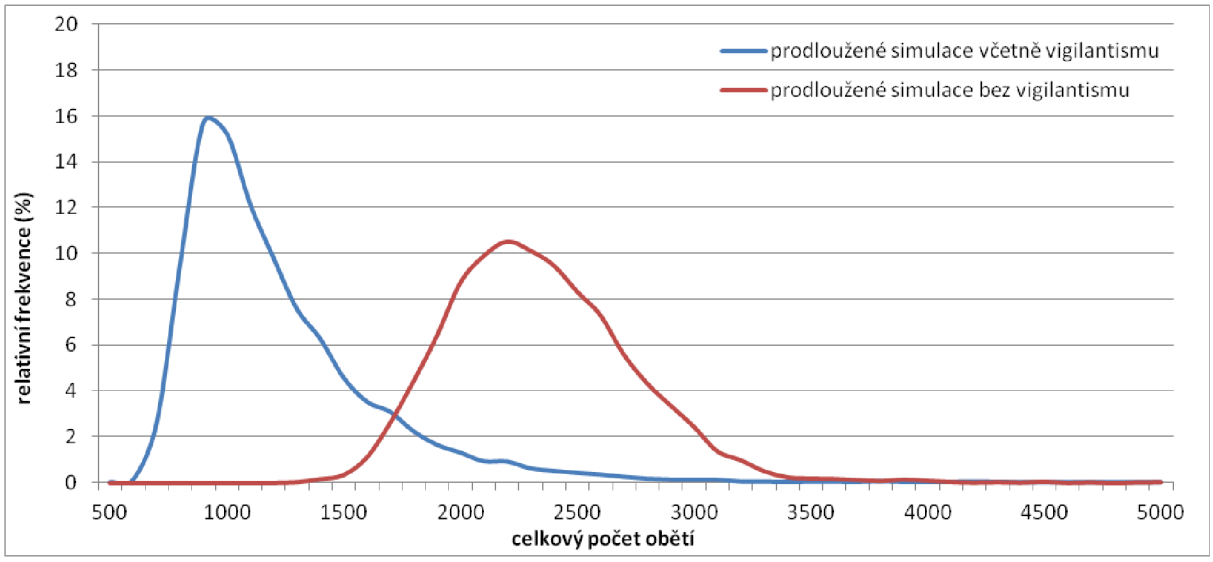
Konečným důsledkem je zhruba dvojnásobný střední počet teroristických útoků i jejich obětí ve srovnání s těmi prodlouženými simulacemi, které kybervigilantismus zahrnují. Nutno podotknout, že i tyto vysoké hodnoty jsou stále nižší, než kdyby byly extrapolovány roky 2015 a 2016. Pokud by v druhé dekádě bylo průměrné roční množství obětí stejné, jako tomu bylo v těchto dvou letech (442 celkem, tedy 221 ročně), byl by konečný výsledek po celých dvaceti letech 2740 obětí, tedy o více než pětinu vyšší, než by naznačovala tato série simulací.

	počet útoků	počet obětí
medián	**507.0**	**2256.5**
průměr	506.4	2300.5
směrodatná odchylka	50.6	437.6
maximum	658.0	10727.9
minimum	306.0	1128.5

Tabulka 7 - statistické hodnoty pro sérii prodloužených simulací bez kybervigilantismu



Graf 32 – komparace histogramů počtů útoků u prodloužených simulací z hlediska vlivu kybervigilantismu



Graf 33 – komparace histogramů počtů obětí u prodloužených simulací z hlediska vlivu kybervigilantismu

Vedle možná až příliš výrazného nárůstu aktivity je druhým důvodem k opatrné skepsi vůči této specifické sérii simulací také velký paralelní nárůst ve vnímání kyberprostoru jako hrozby a korespondující propad „svobody internetu“. Obojí je reakcí modelu právě na onu neefektivitu regulace a cenzury ze strany správců obsahu a ke konci druhé dekády se typicky pohybují kolem 10% od svého maxima, respektive minima.

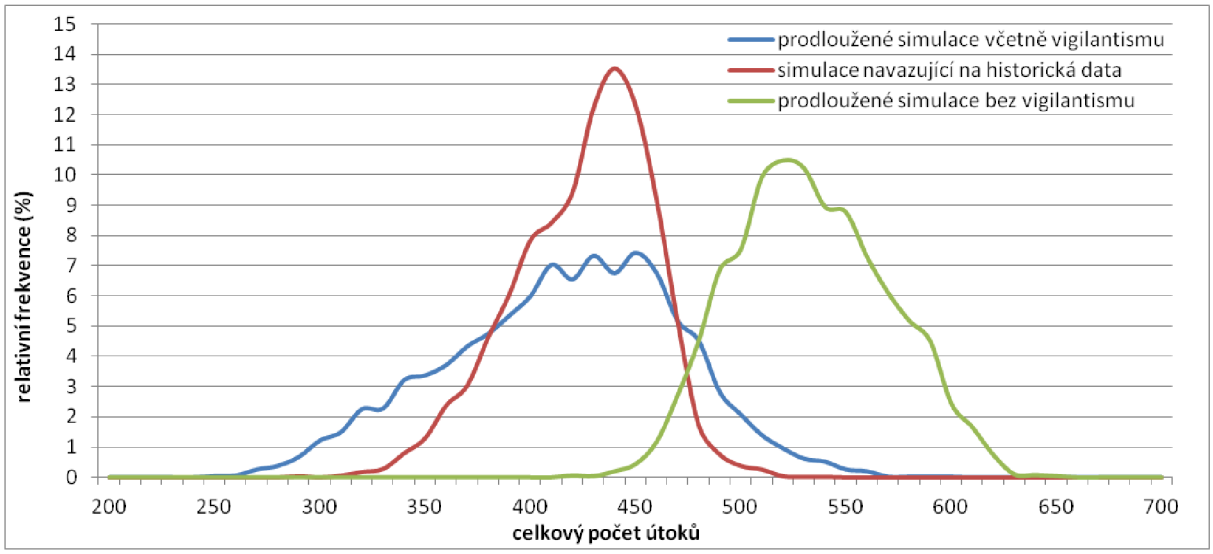
7.4 Návrat džihádistů ze zahraničí

Poslední explorativní režim modelu slouží k odhadu toho, jak by systém mohl zareagovat na budoucí možný a očekávaný návrat džihádistických bojovníků (tzv. fenomén *foreign fighters*), kteří do konfliktních zón (zejména Sýrie a Irák) vycestovali ze Západních zemí. Vzhledem k současné vojenské situaci takzvaného Islámského státu, který je v dlouhodobé teritoriální kontrakci a během léta 2017 ztratil dlouho udržovanou a nespornou suverenitu nad významnými městy Mosul a Rakka, řada autorů očekává, že dojde (či již dochází) ke strategické reorientaci od konvenčního boje a kontroly teritoria směrem k více asymetrickému boji a zejména terorismu. Tento posun v kombinaci s nenaplněním vize kalifátu a návratem již vytrénovaných džihádistů zpět do svých domovin by mohl spustit novou vlnu řízených, a tudíž ničivějších džihádistických teroristických útoků na Západě (srov. Neumann 2014, Lister 2016, Kilcullen 2017, Winter - Clarke 2017, Holmer - Shtuni 2017, Reed – Pohl 2017, Reed – Pohl – Jegerings 2017).

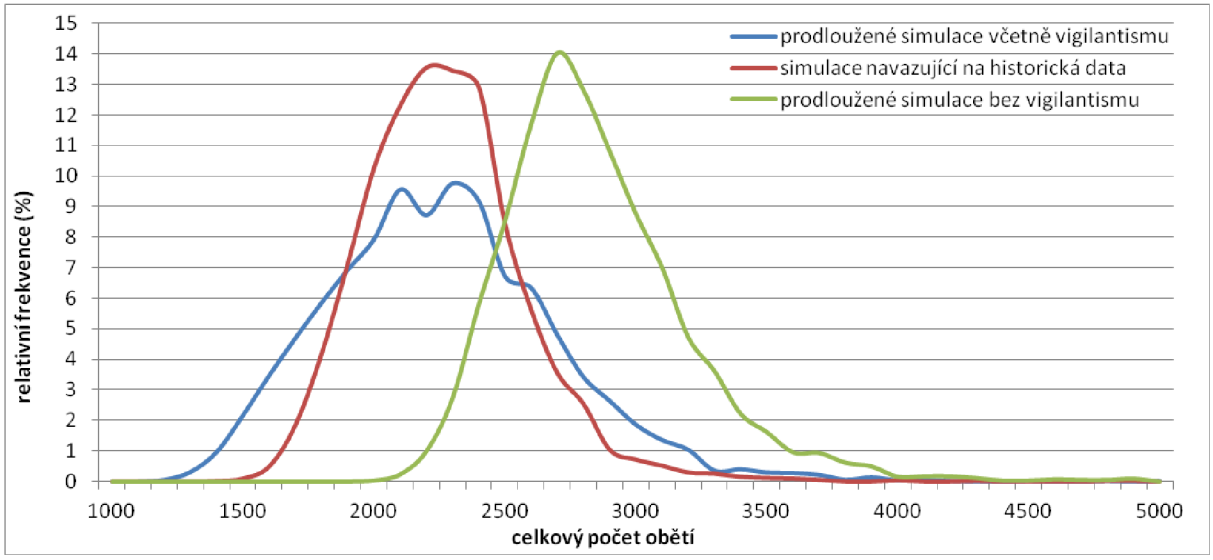
Vzhledem k zaměření této práce a účelu tohoto posledního „experimentu" není nutné a vlastně ani realistické snažit se o precizní stanovení toho, kdy přesně a kolik přesně řízených teroristů se ve formě navrátivších se džihádistů na Západě objeví (natož jak a kam se dostanou). Proto je v zájmu jednoduchosti a srovnatelnosti v modelu v podstatě zrcadlen jejich předchozí vstup, ke kterému došlo na přelomu roku 2014 a 2015, tedy 104 týdnů před koncem první dekády. Druhý vstup je tak stanoven na 104. týden po začátku druhé dekády (tj. přelom let 2018 a 2019, 624. týden simulace), a opět ve velikosti 21. Po této drobné (a jediné) modifikaci modelu jsou do porovnání zahrnuty tři již výše představené režimy – prodloužená základní simulace, která simuluje celých dvacet let se všemi prvky; simulace navazující na historický vývoj, která druhou dekádu rovněž simuluje se všemi prvky modelu; a nakonec prodloužená simulace bez protidžihádistického vigilantismu v kyberprostoru.[69] Komparace těchto tří variant by měla

[69] Přestože by to mohlo být z hlediska symetrie logické, tak simulace, které by navazovaly na historický vývoj a přitom by v nich nefiguroval vigilantismus, zde zahrnuty nejsou. To by totiž představovalo situaci, kdy by do poloviny časového horizontu protidžihádistický vigilantismus standardně působil a najednou po roce 2016, kdy končí referenční vzorek, by vigilantismus přestal hrát v systému roli. Nejednalo by se tudíž o zkoumání vlivu konkrétního prvku na předpokládané chování systému (neboť by se jeho struktura měnila a nedocházelo by k izolování vlivu proměnných) ani o zkoumání jeho budoucího očekávaného chování na základě chování dosavadního. Přinejlepším by se jednalo o imaginární situaci, kdy by byla po roce 2016 tato forma „kybervigilantismu" zcela a náhle vymýcena, což ovšem nekoresponduje s realitou a ani to neodpovídá na žádnou výzkumnou otázku.

posloužit jak k přibližnému odhadu možného budoucího vývoje systému (zůstane-li jeho struktura zachována a nedojde-li k žádným dalším významným exogenním vlivům), tak k posouzení vlivu, jaký má modelovaný kybervigilantismus na reakci systému na takovýto zásah. Vzhledem k experimentálnosti těchto posledních simulací, relativně chabé datové ukotvenosti a také jejich časové náročnosti jsou provedeny na sériích o poloviční velikosti, tedy 5000 běhů.



Graf 34 - komparace histogramů počtů útoků při simulacích s návratem „foreign fighters“



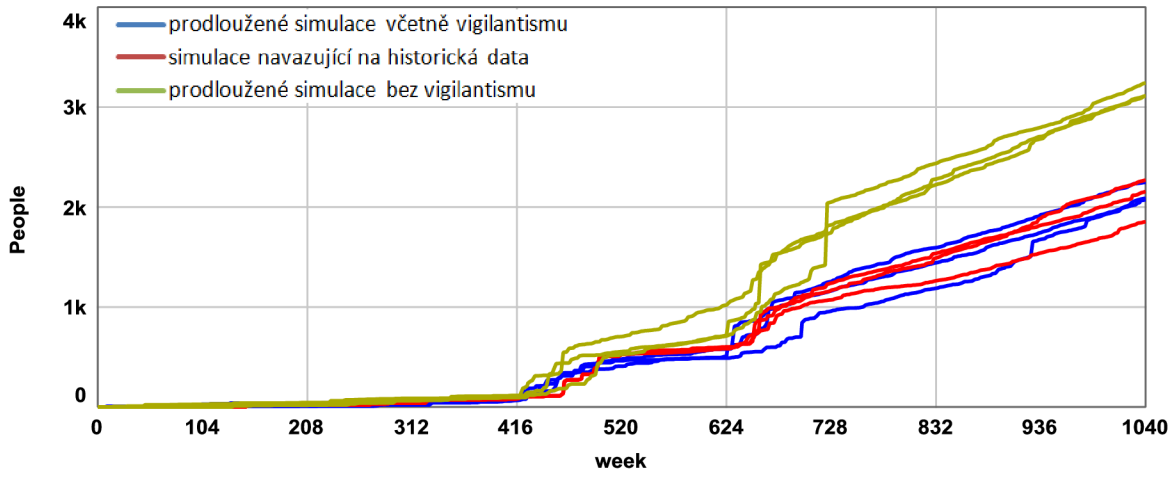
Graf 35 - komparace histogramů počtů obětí při simulacích s návratem „foreign fighters“

	počet útoků			počet obětí		
série:	včetně vigil.	historická	bez vigil.	včetně vigil.	historická	bez vigil.
medián	**416.0**	**425.0**	**526.0**	**2191.5**	**2199.9**	**2743.2**
průměr	411.5	420.2	528.5	2218.5	2221.6	2821.8
směrodatná odchylka	54.9	32.7	36.7	469.0	351.5	825.8
maximum	592.0	533.0	643.0	7605.7	12962.4	47686.8
minimum	245.0	281.0	413.0	1170.6	1336.9	1901.1

Tabulka 8 - statistické hodnoty pro série s návratem „foreign fighters“

Na histogramech i v tabulce je vidět předpokládatelný výsledek, kdy rozdíl mezi sériemi navazujícími na historická data a těmi, které simulují celých dvacet let, je opět především v jejich směrodatné odchylce kolem sdíleného středu. Tento pár simulací je tak konzistentní s výsledky z kapitoly 7.3.4 a přidání druhé vlny řízených teroristů na tom nic nemění. Co se ovšem mění, jsou celkové počty teroristických útoků a jejich obětí, které jsou díky této druhé vlně zhruba dvojnásobné.

Za povšimnutí ovšem stojí, že varianty bez vigilantismu se takto dramatický nárůst díky druhé vlně již nedotýká a pohybuje se spíše v okolí 20% a nikoliv 100%. Modelovaný systém se totiž už blíží k maximální saturaci, kdy se další navyšování viditelnosti skrze endogenní násilí nebo propagandu v kyberprostoru stává velmi obtížným.



Graf 36 - komparativní graf celkových počtů obětí džihádistického terorismu při prodloužených simulacích modelu s návratem „foreign fighters“

8 Závěr

8.1 Zhodnocení modelu

Zcela zásadním pilířem celé práce bylo vytvoření dynamického modelu zkoumaného systému, na kterém by bylo možné analyzovat fungování džihádistického terorismu na Západě, protidžihádistického vigilantismu v kyberprostoru a složité interakce mezi nimi. Vzhledem k tomu, že se jedná o rozsáhlý komplexní a adaptivní sociální systém, bylo přikročeno k metodám z oblasti komputativních sociálních věd, které je možné aplikovat i na tento typ ojedinělých případů s velkým množstvím proměnných (včetně těch „měkkých“, spatně definovatelných a měřitelných). Pro tento účel vznikl zde předkládaný a popsaný model vystavěný především na systémové dynamice, který byl v klíčových bodech navíc doplněn o mocninné zákony a je tak schopen simulací, které v tomto případě představují nejbližší náhražku ideálu pozitivistických přírodních věd – experimentů.

Tím vznikl poměrně netradiční hybridní model, který se od všeobecně převažujících dynamických modelů liší především svojí stochastickou povahou, která si mimo jiné vynucuje odlišný přístup k analýze výsledků, neboť každá jeho jednotlivá simulace je prakticky unikátní a nemusí být vůbec vypovídající o obecném a převažujícím chování systému samotného. Řešením je analyzování celých sérií simulací pro každé jedno nastavení či zkoumaný režim modelu, přičemž pro velikost sérií byla jako kompromis mezi precizností a výpočetní náročností stanovena hodnota 10000 a hlavním posuzovaným parametrem je medián.

Oproti metodologicky a oborově podobným pracím lze za hlavní přínosy tohoto modelu považovat právě kombinaci dvou odlišných komputativních přístupů, která umožňuje zachytit tento hojně zkoumaný systém džihádistického terorismu z nového úhlu pohledu a snad více reprezentativním způsobem, který zahrnuje reakce na jednotlivé dynamicky generované útoky. Dalším pokrokem je pak zapracování dvou částečně oddělených a samostatných typů terorismu (řízený a inspirovaný) a především připojení subsystému reprezentujícího paralelní dění v kyberprostoru, které stále nabývá na důležitosti a jeho praktický dopad na dění ve fyzickém prostoru je sice hojně diskutovaný, ale jen málo vědecky prozkoumaný.

Prvním milníkem takto transdisciplinárně zkonstruovaného modelu byla jeho validace za pomocí historických dat, která byla zkompilována do referenčního vzorku (kapitola 6)

džihádistických teroristických útoků na Západě během sledovaného období 2007 až 2016. Dvěma hlavními zvolenými metrikami, které musel být model schopný replikovat, byly počet uskutečněných útoků a složený počet jejich obětí, který kombinuje zabité i zraněné. Model byl schopen s relativně velkou přesností (1 až 3%) replikovat obě hodnoty pro reálný historický průběh i pro doplňkovou extrapolaci prvních osmi klidnějších let 2007 až 2014.

Dalším krokem navazujícím na validaci modelu bylo provádění „experimentálních" simulací, během kterých byla v modelu vyřazena funkčnost protidžihádistických kybervigilantistů. Díky kontrole této proměnné tak mohl být posouzen, nebo by se snad dalo říci i změřen, vliv tohoto prvku na chování modelu, a tím (za předpokladu, že dostatečně přesně odpovídá své reálné předloze) i systému. Zhodnocení tohoto vlivu, a tím i zodpovězení hlavní výzkumné otázky celé disertační práce se věnuje samostatná podkapitola závěru.

Vedle toho model umožňuje provedení i sérií obdobných, avšak zároveň více spekulativních, simulací, které hledí do budoucna a simulují i následující dekádu a pokrývají tak období 2007 až 2026. Díky snadné modifikovatelnosti modelu se navíc objevují ve dvou variantách, přičemž jedna je pouhým prodloužením délky trvání simulace na dvojnásobek a druhá navíc do modelu zavádí druhou vlnu řízených teroristů, která má reprezentovat často diskutovaný a mnohými očekávaný návrat džihádistů vycestovalých ze Západu. Na těchto simulacích je možné jednak opět sledovat vliv kybervigilantismu, a i když označit je jako prediktivní by bylo nejspíše příliš odvážné, mohou také sloužit jako výhled do následujících let a jako podklad pro úvahy o budoucím chování tohoto systému.

Hlavní slabinou modelu, které se vzhledem ke zkoumané problematice nebylo prakticky možné vyhnout, je relativně velké množství měkkých proměnných, které ztěžují tvorbu modelu i jeho analýzu. V případě budoucích úprav a zásadních revizí modelu by z hlediska jeho chování a přesnosti měla patrně největší přínos jeho konverze na časové kroky po jednom dni, což by bylo sice náročné, ale v zásadě přímočaré, a zapracování i potenciálně zcela neúspěšných teroristických útoků. Velkou výzvou (zejména kvůli nedostatku spolehlivých informací) by potom bylo přidání a diferencování dalších specifických forem kybervigilantismu, konkrétně jejich snah o infiltraci džihádistických komunikačních kanálů. Principiálně strukturálním problémem tohoto modelu, který se projevil zejména v prodloužených dvacetiletých simulacích, je nízká míra adaptivnosti některých jeho prvků, což vedlo k místy až nerealistickým hodnotám, které jsou blíže prozkoumány v následující podkapitole.

8.2 Zhodnocení výsledků

Podrobný popis jednotlivých sérií simulací a jejich výsledků lze nalézt v příslušných kapitolách, nicméně je na místě si je v závěru celkově shrnout a vyhodnotit, co vlastně o modelovaném systému vypovídají. Tabulka č. 9 zachycuje všechny nasimulované nebo z historických dat extrapolované mediány pro počty útoků i obětí a poskytuje tak dobrý podklad pro jejich vzájemné srovnání.

		počet útoků		počet obětí	
		medián	odchylka	medián	odchylka
10 let	referenční historický vzorek	52.0	n/a	525.9	n/a
	extrapolace historie bez eskalace	29.0	n/a	103.8	n/a
	základní simulace/replikace historie	52.0	9.5	523.9	266.9
	základní simulace bez eskalace	30.0	5.3	104.4	45.0
	základní simulace bez vigilantismu	61.0	12.4	559.5	302.3
20 let	extrapolace průměru z celého vzorku	104.0	n/a	1051.8	n/a
	extrapolace průměru z konce vzorku	197.0	n/a	2740.4	n/a
	prodloužená simulace navazující na historii	258.0	30.9	1086.0	200.9
	prodloužená základní simulace	247.0	59.4	1051.5	843.2
	prodloužená simulace bez vigilantismu	507.0	50.6	2256.5	437.6
20 let + FF	prodloužená simulace navazující na historii	425.0	32.8	2199.9	351.5
	prodloužená základní simulace	416.0	54.9	2191.5	469.0
	prodloužená simulace bez vigilantismu	526.0	36.7	2743.3	825.8

Tabulka 9 – přehled hlavních výsledných hodnot ze všech alternativ použitých ve výzkumu

V její levé části je tabulka rozdělena podle jednotlivých skupin, tedy desetiletý horizont, dvacetiletý horizont a nakonec dvacetiletý horizont s přidanými navracejícími se džihádistickými bojovníky za zahraničí („FF“ jako *foreign fighters*). Položky pojmenované jako simulace značí výstupy přímo z modelu tak, jak byly naměřeny z jejich mnohatisícových sérií opakovaných

simulací, a extrapolace značí hodnoty spočítané na základě dat v historickém vzorku (a proto u nich nemá smysl uvádět směrodatnou odchylku).

V této části bude věnována pozornost především prodlouženým simulacím a jejich výsledkům, neboť o přesnosti replikace toho již bylo napsáno dost a vlivu kybervigilantismu na systém se věnuje až další kapitola.

V prvé řadě je nutné upozornit, že jakékoliv hodnocení domnělé „přesnosti“ nebo „důvěryhodnosti“ jednotlivých dopředu hledících simulací je již ze své podstaty neobjektivní a spekulativní, neboť, na rozdíl od těch předchozích, je bohužel nelze (zatím) srovnat s realitou. Tyto výstupy lze srovnat buďto s prostými přímočarými extrapolacemi předchozího historického chování systému (viz tabulka), anebo autorskými intuitivními odhady očekávaného budoucího chování systému. Autorská intuice je ale paradoxně přesně tím, co by komputativní metody v sociálních vědách měly překonávat, namísto aby podle ní byly hodnoceny.[70] Vzhledem k neexistenci dat a subjektivnosti vnímání celého systému lze tedy očekávat, že se budou značně rozcházet individuální hodnocení a názory na to, zda je nějaký výstup modelu příliš velký nebo naopak příliš malý. S vědomím tohoto úskalí je k hodnocení „prediktivních“ simulací přistupováno i zde.

Při pohledu na rozpětí mediánů prodloužených dvacetiletých simulací je zajímavé, že v případě obětí teroristických útoků lze sledovat až podivuhodnou shodu s rozpětím dvou uvedených extrapolací vycházejících z historických dat (přibližně 1050 až 2740). Přitom se v žádném případě nejedná o vlastnost modelu, která by při jeho budování a testování byla cílem nebo jakkoliv sledována. Tuto nápadnou podobnost určitě nelze označit jako náhodnou (neboť cílem modelu samozřejmě je replikovat chování skutečného systému), nicméně je zcela nezamýšleným vedlejším produktem.

V ostrém kontrastu s touto podobností co se počtů obětí týče lze sledovat velký rozdíl co do počtů útoků. I nejméně aktivní prodloužená simulace výrazně převyšuje maximální extrapolovaný počet útoků o 20% a v nejhorších případech je to více než dvojnásobně. Zatímco extrapolace nerozlišují mezi typy teroristických útoků, v modelu je tento rozdíl způsoben velkým nárůstem podílu inspirovaných útoků (tj. minimálně organizovaných a s minimem obětí), který je poháněn radikalizací společně s pokračující proliferací a stoupajícím vlivem informačních a komunikačních

[70] Bohužel jedinou zcela exaktní a zároveň extrémně nepraktickou variantou by bylo výstupy hodnotit až zpětně, tedy po roce 2026.

technologií. V roce 2016 sice lze pozorovat větší podíl těchto útoků oproti roku 2015 (typicky útoky nožem nebo vozidlem na hlídkující vojáky či policii), nicméně z takto krátkého časového úseku a malého množství dat rozhodně nelze vyvozovat celkový trend, natož jej sebevědomě projektovat na dalších 10 let dopředu.

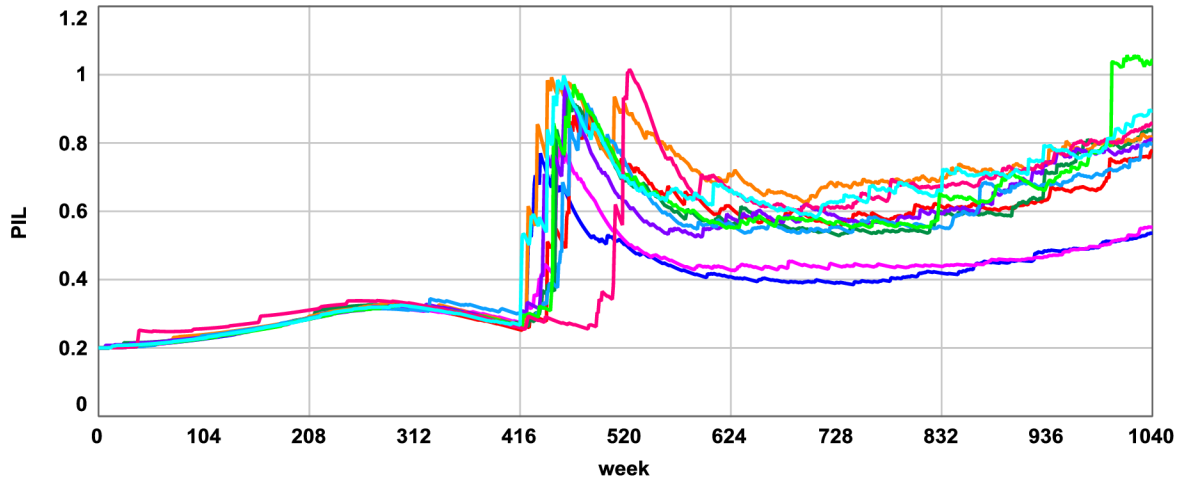
Intuitivně, pod vlivem událostí posledních let [71] a s vědomím potenciálu internetu a kyberprostoru obecně je možné (ale nikoliv nutné) výsledné počty obětí základních simulací považovat za realistické a počty útoků za poněkud nadsazené. Typické chování těchto simulací je pomalý a postupný návrat ze současné vyhrocené situace zpět k nižším hodnotám, přičemž výsledný pokles aktivity v modelu je o poznání pomalejší než jeho prvotní, až skokový, nárůst. I tak se zdá být výsledné simulované tempo průměrně dvaceti džihádistických teroristických útoků ročně během druhé dekády poměrně vysoké.

V praxi budou mít významný vliv i exogenní vlivy, neboť relativní úspěch či neúspěch entit jako je takzvaný Islámský stát nepochybně ovlivňuje lákavost džihádismu i sílu jeho propagandy. Klíčovou proměnnou, která z hlediska modelu také leží mimo jeho kauzální hranice, je potenciální vstup dalších řízených teroristů, kteří jsou díky své organizovanosti a výcviku schopni provádět daleko ničivější útoky, a tím také inspirovat další následovníky a imitátory. Ze simulací vyplývá poměrně silná zpětná vazba a potenciální úspěch těchto vracejících se džihádistů (respektive selhání bezpečnostních opatření, které jim v tom mají zabránit) by měl dalekosáhlé důsledky a oddálil by „zklidnění“ systému o několik dalších let, čímž by vlastně došlo ke znásobení výsledných obětí. V konečném důsledku tak nejde jen o to předejít pouze přímým obětem těchto navrátivších se džihádistů, ale také zabránit následné kaskádě dalších, byť pravděpodobně menších, útoků, který by jejich viditelný úspěch nejspíše spustil. Nicméně i v tomto případě se simulované frekvence útoků jeví jako snad až příliš vysoké.

Příčinou tohoto chování modelu při prodloužených simulacích je jeho již zmiňovaná nízká adaptibilita na rostoucí roli informačních a komunikačních technologií. Zatímco s postupným úbytkem velkých teroristických útoků ve střednědobém horizontu klesá viditelnost a radikalizační potenciál džihádismu, tak v dlouhodobém horizontu nezastavitelně roste vliv digitální propagandy

[71] Počet džihádistických teroristických útoků za první polovinu roku 2017 a dosavadní množství jejich obětí rozhodně nepoukazují na zvrácení modelovaného trendu. Po velmi povrchním průzkumu a přibližných výpočtech se lze za těchto 6 měsíců (tj. bez útoku v Barceloně) dopracovat k asi 9 teroristickým útokům a 65 přepočítaným obětem. Po zdvojnásobení vyjdou hodnoty 18 a 130, které předběžně poukazují na vyšší množství útoků a nižší počty obětí než je průměr za roky 2015 a 2016, který činí 14 a 221.

a v modelu se nenachází žádný jiný mechanismus jak se s tímto vyrovnávat, než posilování digitální cenzury a snižovaní svobody na internetu. Důvodem této absence je jednoduše to, že v současnosti žádný takový alternativní mechanismus není patrný a jak to bude vypadat v budoucnu, není známo. Konečným důsledkem je, že i za absence dalších exogenních vlivů má model ke konci druhé dekády tendenci samovolně se navracet k vyšší viditelnosti (viz graf 37), a tím i generovat větší množství inspirovaných teroristických útoků.



Graf 37 – průběh viditelnosti džihádismu během deseti základních prodloužených simulací

Přestože tato část modelu je tedy dostatečně přesná pro simulace první dekády a zde produkované chování relativně dobře zachycuje současnou realitu, je velmi pravděpodobné, že pod rostoucím náporem využívání kyberprostoru džihádismem (anebo jakoukoliv jinou formou extremismu) v budoucnu dojde ke změnám v její struktuře nebo alespoň k posilnění vlivu prvků, které zde byly pro jejich malý současný dopad na chod zkoumaného systému opomenuty (což může být i něco tak prozaického a zároveň vágního jako rostoucí otrlost nebo apatie společnosti vůči tomuto typu obsahu). Na druhou stranu je třeba si uvědomit, že tento konečný stav modelu, kdy jediným a zároveň nedostatečným „řešením“ tohoto problému je stále se stupňující digitální cenzura, je sice velmi neatraktivní, patrně nežádoucí, ale zároveň zcela možnou eventualitou.

8.3 Role vigilantismu

Hlavním cílem celé práce bylo prozkoumat vliv kybervigilantismu na džihádistický terorismus na Západě. Tento záměr také určoval směřování konstruovaného modelu, jeho vnitřní strukturu i kauzální hranici kolem něj. Hlavním prvkem této analýzy bylo provedení tří sérií simulací, u nichž byl oproti základnímu modelu odstraněn vliv kybervigilantismu, díky čemuž pak mohlo dojít k jejich vzájemnému srovnání (viz tabulka 10).

		počet útoků		počet obětí	
		medián	odchylka	medián	odchylka
10 let	základní simulace/replikace historie	52.0	9.5	523.9	266.9
	základní simulace bez vigilantismu	61.0	12.4	559.5	302.3
	nárůst, zaokrouhleno	17.3 %	30.5 %	6.7 %	13.3 %
20 let	prodloužená základní simulace	247.0	59.4	1051.5	843.2
	prodloužená simulace bez vigilantismu	507.0	50.6	2256.5	437.6
	nárůst, zaokrouhleno	105.2 %	- 15.2 %	114.6 %	- 48.1 %
FF	prodloužená základní simulace	416.0	54.9	2191.5	469.0
	prodloužená simulace bez vigilantismu	526.0	36.7	2743.3	825.8
	nárůst, zaokrouhleno	26.4 %	- 33.2 %	25.2 %	76.1 %

Tabulka 10 - přehled výsledků pro páry simulací včetně a bez kybervigilantismu

U všech tří párů sérií simulací došlo po odstranění kybervigilantismu k měřitelnému navýšení teroristické aktivity v modelu z hlediska počtů džihádistických útoků i jejich obětí. Nicméně velikost tohoto rozdílu se velmi významně lišila podle kontextu modelu a jeho výchozího nastavení.

Při standardních simulacích modelu na deset let byl pozorován nárůst především v počtu útoků, což odpovídá předpokladu, že hlavním konečným účinkem modelovaného kybervigilantismu je brzdění radikalizace inspirovaných teroristů. Tomu odpovídá i o poznání menší nárůst v počtech obětí, neboť tyto navíc generované útoky většinou patří k těm velmi malým. Při porovnání nárůstu obou mediánů se lze dobrat k tomu, že by jim průměrně odpovídaly útoky o čtyřech obětech, což lze považovat za realistické.

Nejextrémnější nárůst bylo možné pozorovat u základní simulace prodloužené na dvacet let. Zde obě hlavní metriky poskočily na více než dvojnásobek, což v tomto případě spíše než na enormní roli kybervigilantismu poukazuje na to, že model s touto konkrétní strukturou nelze takto jednoduše protáhnout do dvojnásobného časového horizontu. Kvůli implementaci vztahu mezi kybervigilantismem a správci digitálního obsahu v modelu totiž dochází k systémovému chování známému jako „přesun břemene“ (*shifting the burden to the intervenor,* viz konec kapitoly 4.1.3), kdy dochází k zaostávání výkonnosti a kapabilit jednoho prvku či aktéra kvůli intervencím jiného prvku či aktéra, který se snaží ovlivnit lokální chování systému pro ně žádoucím směrem. Zde jsou tím intervenujícím prvkem kybervigilantisté a tím zaostávajícím jsou právě zprostředkovatelé obsahu a provozovatelé sociálních sítí. Díky těmto intervencím (v kombinaci s inherentní obtížností úkolu a jejich neochotou riskovat, viz kapitola 3.4) dochází ke snižování tlaku na jejich vlastní protidžihádistické aktivity, neboť část tohoto úkolu (zejména vyhledávání, identifikaci a často i odstranění či zablokování přístupu, viz kapitola 3.3) vlastně dělají za ně sami vigilantisté.

Současný modelovaný stav tak reprezentuje situaci, kdy tento úkol oba prvky sdílejí, přičemž vigilantismus na případný vzestup džihádismu reaguje mnohem rychleji a agresivněji (a mimozákonně), čímž vlastně umožňuje pomalejší a opatrnější spouštění legitimních prostředků k regulování a cenzurování tohoto subjektivně nežádoucího obsahu. V okamžiku, kdy je vigilantismus z modelu zcela odstraněn, dochází k výraznějšímu zaostávání za aktivitami džihádistů v kyberprostoru, protože „atrofovaní“ poskytovatelé služeb nejsou schopni dostatečně rychle a silně reagovat na dramatické výkyvy v systému způsobené generovanými útoky nebo exogenními zásahy. Na prudký nárůst výskytu džihádistické propagandy (a opět by to platilo i pro jakýkoliv jiný typ extremismu) nejsou schopni dostatečně pružně zareagovat, protože změna těchto procesů a budování nových kapacit jim trvá příliš dlouho.

V druhé simulované dekádě se tento nedostatek navíc spojí s neutuchajícím a ničím nevyvažovaným růstem vlivu informačních a komunikačních technologií (viz předchozí podkapitola), načež tato kombinace vyústí v nerealisticky vysoké počty teroristických útoků i obětí. V případě simulací, které navíc obsahují i úspěšný návrat džihádistů ze zahraničí, je relativní nárůst menší, neboť model se díky vyšší průběžné aktivitě způsobené druhou vlnou řízených teroristů dříve dostane do stavu, kdy je viditelnost džihádismu maximálně potírána, a je proto nepřítomností vigilantismu postižen relativně méně.

Pokud by situace dospěla do takto kritického stavu ve skutečnosti, bylo by logické očekávat, že by se i sami poskytovatelé přizpůsobili a naučili pružně reagovat. Motivací pro tuto změnu by nejspíše byl nejen stupňující se tlak ze strany politiků a státních institucí (který již existuje), ale navíc i od jejich vlastních uživatelů. V modelu by tak bylo teoreticky možné přidat nějakou zpětnou vazbu, která by působila na rychlost této adaptace a akcelerovala by schopnost těchto aktérů působit proti džihádistické propagandě a podobným materiálům v kyberprostoru za podmínek, kdy viditelnost džihádismu překročí nějakou únosnou mez. Momentálně ale není podle čeho takovou vazbu modelovat, natož vůbec odhadnout její sílu nebo rychlost.

Do budoucna se jako jedna z možností jeví využití umělé inteligence k automatickému a okamžitému vyhledávání, rozpoznávání a odstraňování nežádoucího obsahu (Greenberg 2017a, Slack Alice 2017). Nicméně v současnosti mají tyto technologie přinejlepším pomocnou úlohu a nedávná historie ukázala, že řešení tohoto typu mohou mít i nezamýšlené důsledky ve formě ovlivňování mínění uživatelů nebo poškození legitimních uživatelů. Jak rychle nebo zda vůbec dojde k jejich nasazení a jaké další technické, politické nebo etické důsledky bude rozšíření těchto technologií mít, ukáže teprve budoucnost, přičemž lze očekávat, že významně ovlivní chod zde zkoumaného systému.

Neopomenutelnou a dosud nevyřešenou bezpečnostní a etickou otázkou je také to, zda je taková cenzura ve formě odstraňování obsahu nebo blokování uživatelských účtů vůbec žádoucí. Na jedné straně dochází ke snížení viditelnosti a radikalizačního potenciálu džihádismu, ale na druhou stranu se jedná o potenciální zdroj informací, které mohou vést k identifikaci útočníků nebo v krajních případech i zmaření plánovaných útoků. Kvantifikaci tohoto fenoménu však bohužel stále brání akutní nedostatek spolehlivých dat.

Na úplný závěr se hodí i zvážit, zda je vůbec vhodné kybervigilantismus považovat za fenomén v boji proti džihádismu celkově prospěšný, a to bez ohledu na povzbudivé výsledky simulací, které tomu nasvědčují. Je totiž zapotřebí vzít v potaz širší kontext, například vedlejší oběti postižené jen kvůli jejich jazykové nebo náboženské podobnosti. Dále dochází k (pro vigilantismus typickému) podrývání legitimních autorit a podpoře kultury pohybující se přinejlepším na hraně zákona (ale většinou spíše až za ní). Nakonec kybervigilantismus také nepřímo přispívá k pokračující neefektivitě ze strany provozovatelů právě těch platforem, které jsou využívány pro šíření obsahu, který se oni sami snaží potírat.

9 Přílohy

9.1 Export rovnic modelu

```
{ VERSION 1.3.1 }

{ INITIALIZATION EQUATIONS }
: s Attack_Counter = 0
    UNITS: 1
: s Curating_Ability = 0
    UNITS: PIL
: s Cybervigilantes = 0
    UNITS: people
: s Directed_Terrorists = 0
    UNITS: people
: s Eliminated_Terrorists = 0
    UNITS: people
: c INITIAL_TOTAL_POPULATION = 885e6
    UNITS: people
: c BASE_SYMPATHIZERS_FRACTION = 0.0013
    UNITS: 1
: c INITIAL_PIL = 0.1
    UNITS: PIL
: s Online_Presence = INITIAL_PIL
    UNITS: PIL
: S Public_Impact = INITIAL_PIL
    UNITS: PIL
: c visibility = Online_Presence+Public_Impact
    UNITS: PIL
: c CAUSE_APPEAL = 1
    UNITS: 1/PIL
: s Sympathizers =
INITIAL_TOTAL_POPULATION*BASE_SYMPATHIZERS_FRACTION*visi
bility*CAUSE_APPEAL
    UNITS: people
: c TERRORISTS_FRACTION = 0.0003
    UNITS: 1
: s Inspired_Terrorists =
Sympathizers*TERRORISTS_FRACTION
    UNITS: people
: s Internet_Freedom = 0.5
    UNITS: 1
: s Total_Population = INITIAL_TOTAL_POPULATION
    UNITS: people
: c IT_POP_FRACTION = 0.02
    UNITS: 1
: s IT_Lit_Pop = Total_Population*IT_POP_FRACTION
    UNITS: people
: s Perceived_Online_Threat = INITIAL_PIL
    UNITS: PIL
: s Total_Casualties = 0
    UNITS: People
: c CURATING_DELAY = 52
    UNITS: week
: c PRESENCE_THRESHOLD = 0.2
    UNITS: PIL
: c MAX_PIL = 1
    UNITS: PIL
: f curating_adoption = ((MAX_PIL-
Curating_Ability)^2/MAX_PIL^2)*SMTH3(Online_Presence-
PRESENCE_THRESHOLD, CURATING_DELAY)/(CURATING_DELAY/10)
    UNITS: PIL/week
: c ATTACK_SEED_D = RANDOM(0, 100)+13
    UNITS: 1
: c ATTACK_SEED_I = RANDOM(0, 100)
    UNITS: 1
: c SCALE_SEED_D = ROUND(1/RANDOM(0, 1000)^(1/2)*42)
    UNITS: people
: c SCALE_SEED_I = ROUND(1/RANDOM(0, 1000)^(1/8)*7)-2
    UNITS: people
: c SEVERITY_SEED_D = RANDOM(0, 1)
    UNITS: 1
: c SEVERITY_SEED_I = RANDOM(0, 1)
    UNITS: 1
: c regime_enforcement =
SMTH3((inspired_attack_scale+directed_attack_scale)*ENFO
RCEMENT_RESPONSE,  ENFORCEMENT_DELAY,  0.005)
    UNITS: 1
: c POLICY_RESPONSE = 0.1
    UNITS: 1/PIL
: c regime_policies =
SMTH3(POLICY_RESPONSE*Public_Impact, POLICY_DELAY)
    UNITS: 1
: c AT1 = 1
    UNITS: week
: c SWITCH = 1
    UNITS: 1
: c BASE_CYBERVIGILANTES_FRACTION = 2e-5
    UNITS: 1/PIL
: f activisation =
(IT_Lit_Pop*BASE_CYBERVIGILANTES_FRACTION*(IF SWITCH=2
THEN 0 ELSE 1)*MAX(0, (visibility-PRESENCE_THRESHOLD))-
Cybervigilantes)/AT1
    UNITS: people/week
: c IMPACT_PER_CASUALTIES = 0.15
    UNITS: PIL/people*week
: c HISTORICAL_CASUALTIES = TIME
    UNITS: people/week
: c SCALING_EXPONENT = 2.02
    UNITS: 1
: c CASUALTIES_PER_SEVERITY = 1
    UNITS: people/severity
: c SEVERITY_PER_DIRECTED_TERRORIST = 8.6
    UNITS: severity/people
: c ATTACK_FREQUENCY_COEFICIENT = 99
    UNITS: 1
: c directed_attack_scale = IF
(ATTACK_SEED_D>ATTACK_FREQUENCY_COEFICIENT)    THEN MIN(
SCALE_SEED_D, Directed_Terrorists)/AT1    ELSE 0
    UNITS: people/week
: c directed_casualties =
SEVERITY_PER_DIRECTED_TERRORIST*directed_attack_scale
*CASUALTIES_PER_SEVERITY*
(1/SEVERITY_SEED_D)^(1/SCALING_EXPONENT)
    UNITS: People/week
: c SEVERITY_PER_INSPIRED_TERRORIST = 1.6
    UNITS: severity/people
: c WERTHER_STRENGTH = 0.19
    UNITS: 1/PIL
: c werther_effect = visibility*WERTHER_STRENGTH
    UNITS: 1
: c inspired_attack_scale = IF
ATTACK_SEED_I>(ATTACK_FREQUENCY_COEFICIENT-
werther_effect*Inspired_Terrorists/SCALE_SEED_I)    THEN
MIN(SCALE_SEED_I, Inspired_Terrorists)/AT1    ELSE 0
    UNITS: people/week
: c inspired_casualties =
SEVERITY_PER_INSPIRED_TERRORIST*inspired_attack_scale
*CASUALTIES_PER_SEVERITY*
(1/SEVERITY_SEED_I)^(1/SCALING_EXPONENT)
    UNITS: People/week
: f casualties_per_week = IF (SWITCH=3 AND TIME<520)
THEN  (HISTORICAL_CASUALTIES)       ELSE
(directed_casualties+inspired_casualties)
    UNITS: people/week
: c impact_generated =
casualties_per_week*IMPACT_PER_CASUALTIES
    UNITS: PIL
: c AT_PIL = 52/4
    UNITS: week
: f change_in_impact_level = MIN(    (MAX_PIL-
Public_Impact)/AT1    ,     (impact_generated-
Public_Impact)       *(Public_Impact*(MAX_PIL-
Public_Impact))/MAX_PIL^2 /AT_PIL)
    UNITS: PIL/week
: c TECHNOLOGY_LEVEL = 1+RAMP(0.1/52, 0)
```

```
    UNITS: 1
: c AT_EDU = 3*52
    UNITS: week
: f education =
(Total_Population*IT_POP_FRACTION*TECHNOLOGY_LEVEL-
IT_Lit_Pop)/AT_EDU
    UNITS: people/week
: c REGULATION_FORCE = 3
    UNITS: 1/PIL
: c IT_regulation =
Perceived_Online_Threat*REGULATION_FORCE
    UNITS: 1
: c AT_IF = 52
    UNITS: week
: c MAX_IF = 1
    UNITS: 1
: f IF_change = ((MAX_IF-
(IT_regulation/TECHNOLOGY_LEVEL))-Internet_Freedom)
*(Internet_Freedom*MAX_IF-
Internet_Freedom^2)/(AT_IF*MAX_IF^2)
    UNITS: 1/week
: c PERFORMANCE_PER_SYMPATHIZER = 2.5e-7
    UNITS: PIL/people/week
: c sympathizers_performance_total =
Sympathizers*IT_POP_FRACTION*TECHNOLOGY_LEVEL*PERFORMANC
E_PER_SYMPATHIZER
    UNITS: PIL/week
: c PERFORMANCE_PER_VIGILANTE = 1e-5
    UNITS: PIL/people/week
: c vigiliantes_performance_total =
Cybervigilantes*PERFORMANCE_PER_VIGILANTE
    UNITS: PIL/week
: c BASE_DECAY_RATE = 0.004
    UNITS: 1/week
: c CURATING_EFFECTIVENESS = 0.002
    UNITS: 1/week
: c decay_and_curating =
BASE_DECAY_RATE*Online_Presence+(Curating_Ability*CURATI
NG_EFFECTIVENESS)/Internet_Freedom
    UNITS: PIL/week
: f online_presence_change =
(sympathizers_performance_total-
vigiliantes_performance_total-
decay_and_curating)*(MAX_PIL-Online_Presence)/(MAX_PIL)
    UNITS: PIL/week
: c AT_POT = 1
    UNITS: week
: c WEEKLY_CYBERDAMAGE_PER_IT_POP = 1e-10
    UNITS: PIL/people
: c cyberdamage =
WEEKLY_CYBERDAMAGE_PER_IT_POP*IT_Lit_Pop*TECHNOLOGY_LEVE
L
    UNITS: PIL
: f POT_change = ((cyberdamage+Online_Presence)-
Perceived_Online_Threat)*(MAX_PIL-
Perceived_Online_Threat)/MAX_PIL  /AT_POT
    UNITS: PIL/week
: c AT_POP = 13
    UNITS: week
: f sympathizers_change =
(CAUSE_APPEAL*Total_Population*visibility*BASE_SYMPATHIZ
ERS_FRACTION-Sympathizers) /AT_POP
    UNITS: People/week
: c GROWTH_RATE = 0.0022/52.18
    UNITS: 1/week
: c population_growth = Total_Population*GROWTH_RATE
    UNITS: people/week
: f total_population_change = population_growth -
casualties_per_week
    UNITS: people/week
: f attack_occurences = IF (casualties_per_week>0)
THEN 1    ELSE 0
    UNITS: 1/week
: c ELIMINATIONS_PER_PERP = 0.77
    UNITS: 1
: c INSERTION = PULSE(21, 416) + PULSE(21,  624)*0
    UNITS: people/week
: f direction = IF SWITCH>0 THEN INSERTION ELSE 0
    UNITS: People/week
: f directed_elimination =
regime_enforcement*Directed_Terrorists/AT1 +
directed_attack_scale*ELIMINATIONS_PER_PERP
    UNITS: People/week
: c PERSUASION = 4e-6
    UNITS: 1/PIL
: c INS_AT = 1
    UNITS: week
: f inspiration =
Sympathizers*visibility*PERSUASION/(1+regime_policies)/I
NS_AT
    UNITS: People/week
: f inspired_elimination =
regime_enforcement*Inspired_Terrorists/AT1 +
inspired_attack_scale*ELIMINATIONS_PER_PERP
    UNITS: People/week
: c ENFORCEMENT_DELAY = 52
    UNITS: week
: c ENFORCEMENT_RESPONSE = 0.01
    UNITS: week/people
: c POLICY_DELAY = 208
    UNITS: week
: c "S-VAR" = 0
    UNITS: 1

{ RUNTIME EQUATIONS }
: s Attack_Counter(t) = Attack_Counter(t - dt) +
(attack_occurences) * dt
    UNITS: 1
: s Curating_Ability(t) = Curating_Ability(t - dt) +
(curating_adoption) * dt
    UNITS: PIL
: s Cybervigilantes(t) = Cybervigilantes(t - dt) +
(activisation) * dt
    UNITS: people
: s Directed_Terrorists(t) = Directed_Terrorists(t - dt)
+ (direction - directed_elimination) * dt
    UNITS: people
: s Eliminated_Terrorists(t) = Eliminated_Terrorists(t -
dt) + (directed_elimination + inspired_elimination) * dt
    UNITS: people
: s Online_Presence(t) = Online_Presence(t - dt) +
(online_presence_change) * dt
    UNITS: PIL
: S Public_Impact(t) = Public_Impact(t - dt) +
(change_in_impact_level) * dt
    UNITS: PIL
: s Sympathizers(t) = Sympathizers(t - dt) +
(sympathizers_change - direction - inspiration) * dt
    UNITS: people
: s Inspired_Terrorists(t) = Inspired_Terrorists(t - dt)
+ (inspiration - inspired_elimination) * dt
    UNITS: people
: s Internet_Freedom(t) = Internet_Freedom(t - dt) +
(IF_change) * dt
    UNITS: 1
: s Total_Population(t) = Total_Population(t - dt) +
(total_population_change) * dt
    UNITS: people
: s IT_Lit_Pop(t) = IT_Lit_Pop(t - dt) + (education -
activisation) * dt
    UNITS: people
: s Perceived_Online_Threat(t) =
Perceived_Online_Threat(t - dt) + (POT_change) * dt
    UNITS: PIL
: s Total_Casualties(t) = Total_Casualties(t - dt) +
(casualties_per_week) * dt
    UNITS: People
: c visibility = Online_Presence+Public_Impact
    UNITS: PIL
: f curating_adoption = ((MAX_PIL-
Curating_Ability)^2/MAX_PIL^2)*SMTH3(Online_Presence-
PRESENCE_THRESHOLD, CURATING_DELAY)/(CURATING_DELAY/10)
    UNITS: PIL/week
: c ATTACK_SEED_D = RANDOM(0, 100)+13
    UNITS: 1
: c ATTACK_SEED_I = RANDOM(0, 100)
    UNITS: 1
: c SCALE_SEED_D = ROUND(1/RANDOM(0, 1000)^(1/2)*42)
```

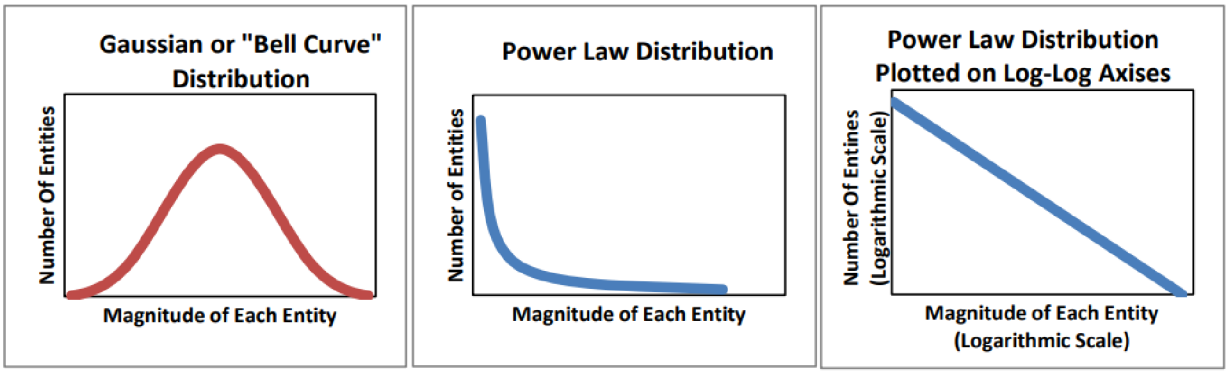
```
    UNITS: people
: c SCALE_SEED_I = ROUND(1/RANDOM(0, 1000)^(1/8)*7)-2
    UNITS: people
: c SEVERITY_SEED_D = RANDOM(0, 1)
    UNITS: 1
: c SEVERITY_SEED_I = RANDOM(0, 1)
    UNITS: 1
: c regime_enforcement =
SMTH3((inspired_attack_scale+directed_attack_scale)*ENFO
RCEMENT_RESPONSE,  ENFORCEMENT_DELAY,  0.005)
    UNITS: 1
: c regime_policies =
SMTH3(POLICY_RESPONSE*Public_Impact, POLICY_DELAY)
    UNITS: 1
: f activisation =
(IT_Lit_Pop*BASE_CYBERVIGILANTES_FRACTION*(IF SWITCH=2
THEN 0 ELSE 1)*MAX(0, (visibility-PRESENCE_THRESHOLD))-
Cybervigilantes)/AT1
    UNITS: people/week
: c HISTORICAL_CASUALTIES = GRAPH(TIME) {...}[72]
    UNITS: people/week
: c directed_attack_scale = IF
(ATTACK_SEED_D>ATTACK_FREQUENCY_COEFICIENT)    THEN MIN(
SCALE_SEED_D, Directed_Terrorists)/AT1    ELSE 0
    UNITS: people/week
: c directed_casualties =
SEVERITY_PER_DIRECTED_TERRORIST*directed_attack_scale
*CASUALTIES_PER_SEVERITY*
(1/SEVERITY_SEED_D)^(1/SCALING_EXPONENT)
    UNITS: People/week
: c werther_effect = visibility*WERTHER_STRENGTH
    UNITS: 1
: c inspired_attack_scale = IF
ATTACK_SEED_I>(ATTACK_FREQUENCY_COEFICIENT-
werther_effect*Inspired_Terrorists/SCALE_SEED_I)    THEN
MIN(SCALE_SEED_I, Inspired_Terrorists)/AT1    ELSE 0
    UNITS: people/week
: c inspired_casualties =
SEVERITY_PER_INSPIRED_TERRORIST*inspired_attack_scale
*CASUALTIES_PER_SEVERITY*
(1/SEVERITY_SEED_I)^(1/SCALING_EXPONENT)
    UNITS: People/week
: f casualties_per_week = IF (SWITCH=3 AND TIME<520)
THEN  (HISTORICAL_CASUALTIES)       ELSE
(directed_casualties+inspired_casualties)
    UNITS: people/week
: c impact_generated =
casualties_per_week*IMPACT_PER_CASUALTIES
    UNITS: PIL
: c AT_PIL = 52/4
    UNITS: week
: f change_in_impact_level = MIN(    (MAX_PIL-
Public_Impact)/AT1    ,     (impact_generated-
Public_Impact)       *(Public_Impact*(MAX_PIL-
Public_Impact))/MAX_PIL^2 /AT_PIL)
    UNITS: PIL/week
: c TECHNOLOGY_LEVEL = 1+RAMP(0.1/52, 0)
    UNITS: 1
: c AT_EDU = 3*52
    UNITS: week
: f education =
(Total_Population*IT_POP_FRACTION*TECHNOLOGY_LEVEL-
IT_Lit_Pop)/AT_EDU
    UNITS: people/week
: c IT_regulation =
Perceived_Online_Threat*REGULATION_FORCE
    UNITS: 1
: f IF_change = ((MAX_IF-
(IT_regulation/TECHNOLOGY_LEVEL))-Internet_Freedom)
*(Internet_Freedom*MAX_IF-
Internet_Freedom^2)/(AT_IF*MAX_IF^2)
    UNITS: 1/week
: c sympathizers_performance_total =
Sympathizers*IT_POP_FRACTION*TECHNOLOGY_LEVEL*PERFORMANC
E_PER_SYMPATHIZER
    UNITS: PIL/week
: c vigiliantes_performance_total =
Cybervigilantes*PERFORMANCE_PER_VIGILANTE
    UNITS: PIL/week
: c decay_and_curating =
BASE_DECAY_RATE*Online_Presence+(Curating_Ability*CURATI
NG_EFFECTIVENESS)/Internet_Freedom
    UNITS: PIL/week
: f online_presence_change =
(sympathizers_performance_total-
vigiliantes_performance_total-
decay_and_curating)*(MAX_PIL-Online_Presence)/(MAX_PIL)
    UNITS: PIL/week
: c cyberdamage =
WEEKLY_CYBERDAMAGE_PER_IT_POP*IT_Lit_Pop*TECHNOLOGY_LEVE
L
    UNITS: PIL
: f POT_change = ((cyberdamage+Online_Presence)-
Perceived_Online_Threat)*(MAX_PIL-
Perceived_Online_Threat)/MAX_PIL  /AT_POT
    UNITS: PIL/week
: f sympathizers_change =
(CAUSE_APPEAL*Total_Population*visibility*BASE_SYMPATHIZ
ERS_FRACTION-Sympathizers) /AT_POP
    UNITS: People/week
: c GROWTH_RATE = 0.0022/52.18
    UNITS: 1/week
: c population_growth = Total_Population*GROWTH_RATE
    UNITS: people/week
: f total_population_change = population_growth -
casualties_per_week
    UNITS: people/week
: f attack_occurences = IF (casualties_per_week>0)
THEN 1    ELSE 0
    UNITS: 1/week
: c INSERTION = PULSE(21, 416) + PULSE(21,  624)*0
    UNITS: people/week
: f direction = IF SWITCH>0 THEN INSERTION ELSE 0
    UNITS: People/week
: f directed_elimination =
regime_enforcement*Directed_Terrorists/AT1 +
directed_attack_scale*ELIMINATIONS_PER_PERP
    UNITS: People/week
: f inspiration =
Sympathizers*visibility*PERSUASION/(1+regime_policies)/I
NS_AT
    UNITS: People/week
: f inspired_elimination =
regime_enforcement*Inspired_Terrorists/AT1 +
inspired_attack_scale*ELIMINATIONS_PER_PERP
    UNITS: People/week

{ TIME SPECS }
STARTTIME=0
STOPTIME=1040
DT=1
INTEGRATION=RK4
RUNMODE=NORMAL
PAUSEINTERVAL=0

{ The model has 93 (93) variables (array expansion in
parens).
  In root model and 0 additional modules with 0 sectors.
  Stocks: 14 (14) Flows: 15 (15) Converters: 64 (64)
  Constants: 40 (40) Equations: 39 (39) Graphicals: 1
(1)
  There are also 30  expanded macro variables.  }
```

[72] Obsah grafické funkce reprezentující historická data o útocích a jejich obětech byl z exportu rovnic odstraněn, protože by zbytečně zabíral příliš mnoho prostoru a pouze kopíruje hodnoty z referenčního vzorku.

9.2 Odkazy ke vzorku teroristických útoků

datum	odkaz
2007-06-30	http://news.bbc.co.uk/2/hi/uk_news/scotland/6257846.stm
2007-11-12	http://www.swissinfo.ch/eng/army-rifle-used-in-islamic-centre-shooting/6248078
2008-12-31	http://www.ynetnews.com/articles/0,7340,L-3648282,00.html
2009-03-20	http://www.cbc.ca/news/world/11-wounded-in-shooting-near-french-school-nursery-1.796017
2009-06-01	http://edition.cnn.com/2011/CRIME/07/25/arkansas.recruiter.shooting/
2009-10-12	https://ctc.usma.edu/posts/the-october-2009-terrorist-attack-in-italy-and-its-wider-implications
2009-11-05	http://www.nbcnews.com/id/33678801/ns/us_news-crime_and_courts/t/gunman-kills-wounds-fort-hood/
2010-05-14	https://www.theguardian.com/uk/2010/nov/03/roshonara-choudhry-jailed-life-attack
2010-12-11	http://www.bbc.co.uk/news/world-europe-11983667
2011-03-02	http://www.washingtonpost.com/wp-dyn/content/article/2011/03/02/AR2011030202651.html
2012-03-15	http://www.worldaffairsjournal.org/article/merah-%E2%80%98untold-story%E2%80%99-french-jihadist-icon http://www.telegraph.co.uk/news/worldnews/europe/belgium/9139693/Imam-killed-in-arson-attack-on-Brussels-mosque.html
2012-03-19	http://www.worldaffairsjournal.org/article/merah-%E2%80%98untold-story%E2%80%99-french-jihadist-icon
2012-07-18	http://www.terrorism-info.org.il/Data/articles/Art_20474/E_029_13_753532921.pdf
2013-04-15	http://edition.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts/
2013-05-22	https://www.theguardian.com/uk-news/2013/dec/19/lee-rigby-killing-woolwich-verdict-convicted-murder http://www.reuters.com/article/us-france-stabbing-idUSBRE94U11M20130531
2013-05-26	http://www.dailymail.co.uk/news/article-2331919/Full-Sutton-Jail-attack-Terror-police-called-prison-warder-held-hostage-Muslim-inmates
2013-11-18	http://www.independent.co.uk/news/world/europe/paris-shootings-suspect-abdelhakim-dekhar-charged-with-attempted-murder-and-kidn
2014-05-24	https://www.theguardian.com/world/2014/jun/01/french-suspect-brussels-jewish-museum-attack-syria
2014-09-24	http://www.nbcnews.com/news/crime-courts/man-beheaded-co-worker-moore-oklahoma-workplace-attack-police-n212396
2014-10-14	http://globalnews.ca/news/1625585/canadian-soldier-struck-by-car-in-quebec-has-died/
2014-10-22	http://www.cbc.ca/news/politics/ottawa-shooting-a-day-of-chaos-leaves-soldier-gunman-dead-1.2808710 http://edition.cnn.com/2014/10/24/us/new-york-police-attacked/ http://www.torontosun.com/2014/10/20/possible-terror-attack-as-soldiers-run-down-in-quebec-parking-lot
2014-12-20	https://www.theguardian.com/australia-news/2014/dec/20/sydney-siege-timeline-how-a-day-and-night-of-terror-unfolded-at-the-lindt-cafe http://www.bbc.com/news/world-europe-30563920
2014-12-21	http://www.bbc.com/news/world-europe-30571911
2015-01-07	http://www.bbc.com/news/world-europe-30708237
2015-02-03	https://www.nytimes.com/2017/02/03/world/europe/louvre-paris-shooting-soldier.html?_r=1
2015-02-14	http://www.bbc.com/news/world-europe-31475803
2015-04-19	https://www.theguardian.com/world/2015/apr/24/french-police-charge-student-links-terrorist-organisation
2015-05-03	http://edition.cnn.com/2015/05/04/us/garland-mohammed-drawing-contest-shooting
2015-06-26	http://www.independent.co.uk/news/world/europe/air-products-france-beheading-attack-suspect-has-killed-himself-authorities-confirm-a
2015-07-16	http://edition.cnn.com/2015/07/16/us/tennessee-naval-reserve-shooting
2015-08-21	http://edition.cnn.com/2015/08/21/europe/france-train-shooting/index.html
2015-09-17	http://www.reuters.com/article/us-germany-shooting-idUSKCN0RH2B920150917
2015-11-02	http://www.abc.net.au/news/2015-10-03/nsw-police-headquarters-gunman-was-radicalised-youth/6825028 http://thehill.com/blogs/blog-briefing-room/news/273524-fbi-student-in-uc-merced-campus-stabbing-inspired-by-terrorist
2015-11-13	http://www.bbc.com/news/world-europe-34818994
2015-12-02	http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html http://www.telegraph.co.uk/news/2016/05/24/leytonstone-tube-attack-man-admits-trying-to-stab-four-people-at/
2016-01-01	http://www.telegraph.co.uk/news/worldnews/europe/france/12077870/Driver-shot-as-he-drove-car-at-troops-guarding-French-mosque.ht
2016-01-07	http://www.telegraph.co.uk/news/worldnews/europe/france/12086901/Paris-police-shoot-dead-knife-wielding-man-live.html
2016-02-11	http://edition.cnn.com/2016/02/12/us/columbus-machete-attack-motive/index.html
2016-02-26	http://www.dw.com/en/from-hanover-to-is-the-case-of-safia-s/a-36094144
2016-03-22	https://www.ict.org.il/UserFiles/ICT-Brussels-Attacks-Mar-16.pdf
2016-04-16	http://www.dw.com/en/german-teens-sentenced-for-sikh-temple-bombing-in-essen/a-38043937
2016-06-12	https://www.nytimes.com/2016/06/13/us/orlando-nightclub-shooting.html https://www.theguardian.com/world/2016/jun/14/french-police-officer-wife-murdered-larossi-abballa-isis
2016-07-14	http://www.bbc.com/news/world-europe-36801671
2016-07-18	https://www.nytimes.com/2016/07/20/world/europe/germany-train-ax-attack.html
2016-07-24	http://edition.cnn.com/2016/07/24/world/ansbach-germany-blast/ http://www.telegraph.co.uk/news/2016/07/26/two-men-with-knifes-take-hostages-in-normandy-church/
2016-08-06	http://www.politico.eu/article/charles-michel-early-indications-charleroi-attack-was-terrorism/
2016-08-19	http://www.independent.co.uk/news/world/europe/strasbourg-rabbi-jewish-stabbing-france-latest-attacker-knife-allahu-akbar-terrorism-a
2016-08-30	http://www.independent.co.uk/news/world/europe/toulouse-attack-man-shouting-im-sick-of-france-stabs-police-officer-in-neck-a7217591
2016-09-17	http://bnonews.com/news/index.php/news/id5142 http://edition.cnn.com/2016/09/17/us/nj-explosive-trash-can/
2016-10-05	http://www.telegraph.co.uk/news/2016/10/05/two-policemen-injured-in-brussels-stabbing-in-jihadi-hotbed-dist/
2216-11-28	http://edition.cnn.com/2016/11/29/us/ohio-state-university-attack/
2016-12-19	http://www.bbc.com/news/world-europe-38377428

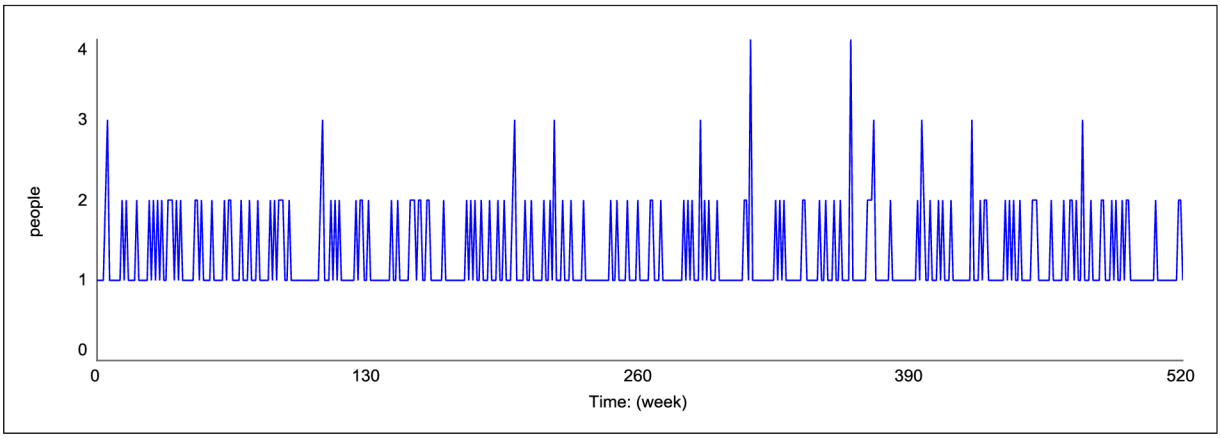
9.3 Grafické srovnání normálního rozdělení a mocninného zákona



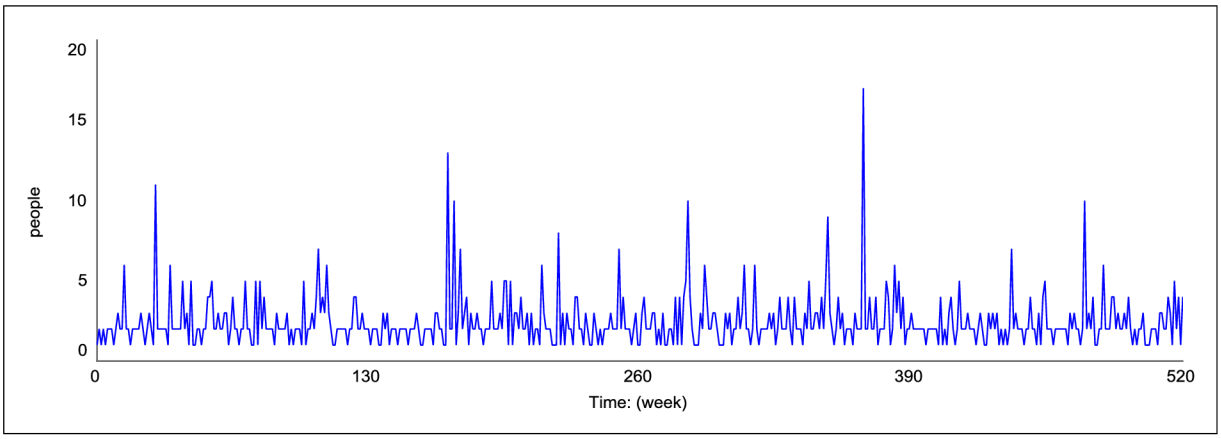
zdroj: Bibighaus 2015: 41

9.4 Ukázky výstupů z pseudonáhodných funkcí generujících počet teroristů podílejících se na teroristickém útoku

Pro inspirované útoky (*SCALE_SEED_I*):

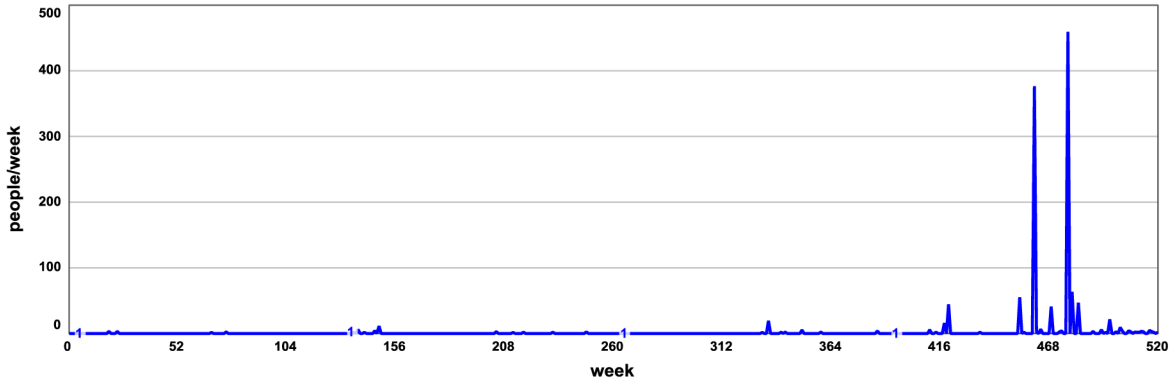


Pro řízené útoky (*SCALE_SEED_D*):

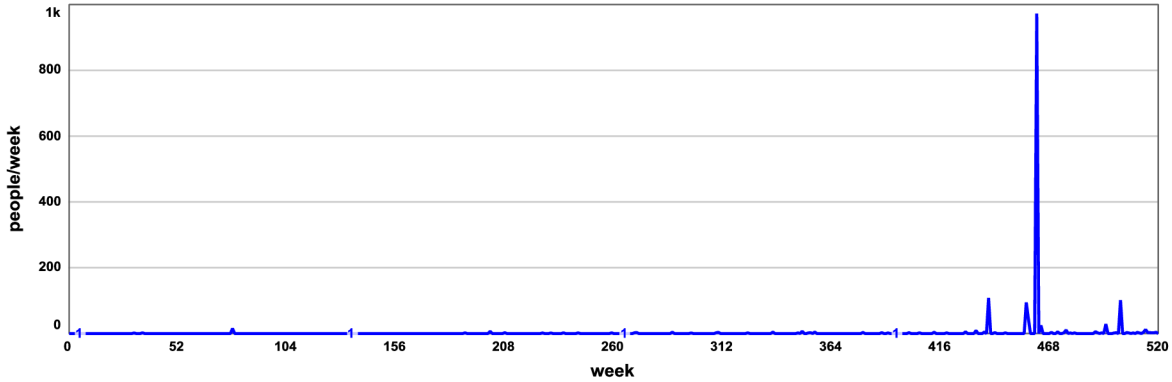


9.5 Ukázky excesivního průběhu základní simulace

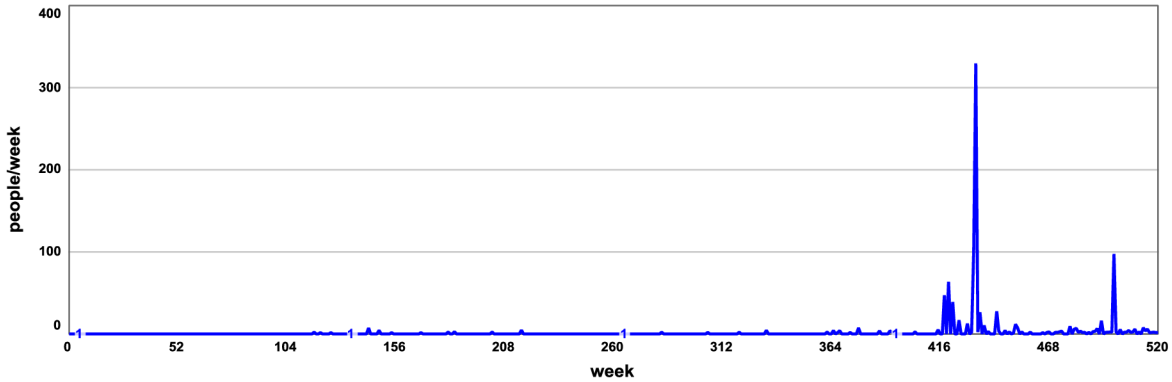
55 útoků, 1291 obětí



66 útoků, 1584 obětí



89 útoků, 1040 obětí



9.6 Výměna mezi americkým vojákem a bojovníkem ISIS

Reddit, 28.11. 2015 - 3.12. 2015, bez úprav.

https://www.reddit.com/r/casualiama/comments/3ulkob/islamic_state_isisisilis_fighter_taking_questions/cxfwiil/

xcommon (námořnictvo USA): "I'm going to drink the kool-aid and give you the benefit of the doubt, that you are telling the truth. I'm a US service-member on a deployment and it kind of fascinates me that I may correspond with someone who is my enemy. I come from Catholic origins but am agnostic/non-practicing. On to my questions:

1. I work with several muslims, and I know two very well. They are great people, smart, kind, funny, confident, and loyal. They denounce the acts of IS, on the grounds of it not being in line with Muslim core-teachings. But mostly that, even if it was, it offends them to the core. When you see the atrocities being committed by your brothers (and possibly you), does it not affect you? Do you see it as justified or necessary? Or do you see nothing wrong with it at all?
2. You don't have to be Sun Tzu to see the writing on the wall. Even if this really was considered to be a war of attrition by IS leaders, none of the great economies are bankrupting themselves in the battle. We spend crazy amounts of money on exercises. We trash loads of ordinance that expire. The war on IS is simply another place to keep our troops sharp and get rid of old ordinance we don't need anymore. The modern world won't attrite before IS ground to dust. What possible end-game can you see? Or is martyrdom your goal?
3. I feel it's important to understand your enemy. I'm familiar with the Torah, Bible, and Quran. I respect your beliefs and your rights to have them. I understand the views of IS, based on their many public releases. Based on your predilection for extremism, it's not possible for you to safely occupy the same land as my friends and family. Because of your willingness to violently impose your will on others, the only thing we can do with you is imprison or eliminate you. There aren't any other options. Do you feel you understand your enemy? Do you understand my mindset and, if so, is my desire to simply raise my family in peace, absent your faith, too much of and impasse for you?
4. You could potentially live next door to me, raise a family, go to your Mosque, live a full and happy life. The only thing you can't do, is hurt and subjugate others, without reprisal and consequences. Ultimately, your ideas, that you could have passed on to your sons and daughters will die with you. Do you have any sense of loss for the life you could have had?

This isn't WW3 for us. You aren't a significant force and you're incapable of occupying a significant country or inflicting significant losses. You're not going to bankrupt us. Our spending is the same regardless of whether or not we're fighting you. Your attacks on civilians only garner patriotism and increase the military ranks of your enemies.

Lastly, I want to thank you for bringing the world closer together. The world's superpowers have been tied together socioeconomically for decades, and now we have a common military goal, potentially paving the way for mutual cooperation, the easing of tensions and possibly even future alliances. How freaking ironic would it be if you guys actually ended up being the harbingers of world peace? lol"

chechlear (ISIS, původně z Holandska, později zabit při náletu): "I've had thousands of questions from thousands of different people (ask.fm/Tumblr) and I must say your series of questions are definitely in my "best" questions list.

Don't get too excited though, I'm going to keep my answers very short and simple.

1. Not everybody who claims to be a Muslim actually understands the core meaning of being a Muslim (in all aspects of life), and thus it's normal for those people to look at us and call us a bunch of barbarians while all that we are doing is implementing the same beliefs they claim to believe in. If they would truly understand Islam and live according to it their attitude towards us would be very different.
2. Nations greater in power and stronger than the United States have been destroyed in the past, they just like yourself thought that they were untouchable, strong and everlasting - but when our Lord Wills it's end game for the United States as a superpower and maybe you'll live long enough to witness it for yourself. And yes our ultimate goal is always Martyrdom for the sake of our Lord, but that could be today or tomorrow or even 20 years from now only God knows.
3. There are many Christians living under the Islamic State, and like you so desire they live in peace and go about in their daily lives. They pay the State Jiziyah once a year depending on their wealth and can reside peacefully in Muslim lands under our protection

without anybody harming them. I've lived most of my life in Europe and fully understand you and your perspective - and I wish we could have a cup of coffee and I could explain it to you in full details but the circumstances are a bit complicated for that scenario :-)

4. True, but I would be the Muslim you desire me to be, not the Muslim my Lord orders us to be, Islam outside of the Islamic State is often politically correct and suffers censorship and other restrictions. Here we live Islam the way our Lord ordered us to live it, and by the Traditions of the Prophet of Islam. And we thank our Lord for that, and are willing to spill our blood for it and that of our families without a second thought.

Ranks will increase and more alliances will be made, we are fully aware of these things and they only increase us in Faith and put a big smile on our face - seeing the whole world slowly assemble against us only adds more conviction to us being on the Right Path, for the enemies of Islam will always assemble and unite against true Islam based on Tawheed and those living under and by it. And regarding these coalitions etc - from the outside they might seem united, yet in their hearts they hate each other and secretly have their own agendas in mind, you should read the Quran, Allah (SWT) mentions it.

By the Will of our Lord and by implementing His Laws which is Justice - we will be those who bring world peace and end corruption wherever we find it"

xcommon: "I respect your convictions and appreciate your openness for discourse.

I apologize if I am misinterpreting your intended message but, your answers seem to be comprised of equal parts dogma and naïveté. You're going to need to ground your thoughts with a little bit more logic if you want them to be taken seriously by anyone non-muslim. I don't believe that anyone with an education is going to give your points merit because you back them up with a quote from a 1400 year old book.

Your belief in the potential for victory seems revolve around the idea that:

1. More people are going to join you. Yes, some may, but not nearly enough. Even if every Muslim the world over joined you, you'd still be outnumbered 2.5:1. And I have a feeling your not going to get that many.
2. US is going to fall at some point. I mean, yeah, maybe. But, when we do go down, it's probably going to be our own fault anyway. Rome fell too, but they crushed plenty of barbarian hordes before that happened. Very few empires fall suddenly, and without symptoms. And none of them we're part of a publicly-traded world economy. The US is probably not going to be leading world superpower forever, but I wouldn't count on us sinking into the ocean tomorrow, or in the next 100 years.
3. Allah will guide you to victory. I can't logically dispute this other than to say that I don't see any evidence to support it.

Generally, people the world over want to be able to make a living, pride for their family, and live in peace. I see you saying that minority faiths live in peace amongst Muslim, but do they really? Are there a lot of Christians fighting along side you in hopes of this 'peace'? I can't imagine anyone being content living as a second-class citizen under what would essentially be a more extreme version of Jim Crow, complete with bigotry, abuse, and additional taxes. If you opened a Mosque in the states right now, you'd be tax exempt, all faiths are.

Again, i respect your convictions as an adversary and appreciate your openness to discuss why you do what you do. But if you and yours ever want to be respected as an actual military force, attacks against civilians have to stop. If you kill a civilian accidentally while you're gunning me down in the street, that's one thing. Collateral damage is what it is and military targets are fair-play; bombing a church or synagogue or shooting a bunch of people while they're trying to enjoy a soccer game is not what a capable and competent military does and those of your ancestors with honor would be ashamed of you. You never answered the question about how the targeting of civilians makes you feel btw."

chechlear: "I'm sure you could write a whole book on how you feel and what you think of us being scum of the earth - but to truly understand us (your enemy in this case) one must start from the pure principals and foundations this religion was built upon.

I would strongly recommend you to read; Al-Wala' wa'l-Bara' According to the Aqeedah of the Salaf, By Shaykh Muhammad Saeed al-Qahtani. (3 parts)

I would also recommend you to listen to some of Anwar al Awlakis lectures regarding the United States, he lived in the US for 21 years and right before he and his 15 year old innocent son got killed by the US left some messages for the people of America.

I pray for your guidance.

10 Zdroje[73]

Ammori, M. – Poellet, K. (2010): „Security versus Freedom on the Internet: Cybersecurity and Net Neutrality.“ *SAIS Review of International Affairs*, Vol. 30, No. 2, p. 51-65. ISSN: 1088-3142

Anderson, E. (2011): „A dynamic model of counterinsurgency policy including the effects of intelligence, public security, popular support, and insurgent experience.“ *System Dynamics Review,* Vol. 27, p. 111–141. DOI: 10.1002/sdr.443

Angwin, J. - Grassegger, H. (2017): “Facebook’s secret rules mean that it’s OK to be anti-Islam, but not anti-gay.” *Ars Technica*, 28.6. 2017. https://arstechnica.com/tech-policy/2017/06/facebooks-opaque-censorship-policy-means-some-attacks-are-ok-others-arent/

Armasu, L. (2017): “Crypto War 3: ‘Five Eyes’ And G20 Nations Plan Renewed Assault On Encryption.” *Tom’s Hardware,* 26.6. 2017. http://www.tomshardware.com/news/fie-eyes-coordinated-assault-encryption,34875.html

Armenia, S. – Cardazzone, A. – Carlini, C. (2014): “Understanding Security Policies In The Cyber Warfare Domain Through System Dynamics.” *Proceedings of the 2014 International Conference of the System Dynamics Society.* http://www.systemdynamics.org/conferences/2014/proceed/papers/P1262.pdf

Armenia, S. – Tsaples, G. (2016): „Individual Behavior as a Defense in the War on Cyberterror: A System Dynamics Approach.“ *Studies in Conflict & Terrorism*, p. 1-24. DOI: 10.1080/1057610X.2016.1249775

Bagot, M. (2017): “Theresa May to urge world leaders to pile pressure on Facebook and social media firms to get tough on terror.” *Mirror*, 26.5. 2017. http://www.mirror.co.uk/news/politics/theresa-urge-world-leaders-pile-10502239

Band, S. R. et al. (2006): *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*. The Defense Personnel Security Research Center. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2006_005_001_14798.pdf

Bakker, E. (2012): *Forecasting the Unpredictable: A Review of Forecasts on Terrorism 2000 - 2012.* International Centre for Counter- Terrorism. https://www.icct.nl/download/file/ICCT-Bakker-Forecasting-the-Unpredictable-July-2012.pdf

[73] Všechny elektronické zdroje ověřeny k 17. září 2017.

Barker, E. - Kelsey, J. (2015): *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. NIST SP 800-90A Rev. 1, National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

Beaumont, P. (2011): "The truth about Twitter, Facebook and the uprisings in the Arab world." *The Guardian*, 25.2. 2011. https://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya

von Behr, I. - Reding, A. - Edwards, C. - Gribbon, L. (2013): *Radicalisation in the digital era*. RAND Corporation. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Bibighaus, D. L. (2015): „How Power-Laws Re-Write The Rules Of Cyber Warfare." *Journal of Strategic Security*, Vol. 8, No. 4, p. 39-52. DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439

Berger, J. M. - Morgan, J. (2015): *The ISIS Twitter Census*. The Brookings Project on U.S. Relations with the Islamic World. https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

Bissell, C. (2007): "The Moniac A Hydromechanical Analog Computer of the 1950s." *IEEE Control Systems,* Vol. 27, No. 1, p. 69-74. ISSN: 1066-033X

Bohorquez, J. C. - Gourley, S. - Dixon, A. R. - Spagat, M. - Johnson, N. F. (2009): "Common ecology quantifies human insurgency." *Nature* Vol. 462, p. 911-914. DOI: 10.1038/nature08631

Borum, R. (2011): "Radicalization into Violent Extremism I: A Review of Social Science Theories." *Journal of Strategic Security,* Vol. 4, No. 4, p. 7-36. ISSN: 1944-0464

Bridgeman, A. (2016): "This Hacker Is Trolling ISIS Twitter Accounts In the Best Way Possible." *CollegeHumor*, 15.6. 2016. http://www.collegehumor.com/post/7038280/this-guy-is-hacking-isis-supporter-twitter-accounts

Brooking, E. T. (2015): "Anonymous vs. the Islamic state." *Foreign Policy*, 13.11. 2015. http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/

Bryant, R. (2001): "What kind of space is cyberspace?" *Minerva - An Internet Journal of Philosophy,* Vol. 5. ISSN 1393-614X

Cain, A. C. - Gonzalez, B. (2017): “Twitter Must Do More to Block ISIS.” *The New York Times*, 13.1. 2017. https://www.nytimes.com/2017/01/13/opinion/twitter-must-do-more-to-block-isis.html

Callimachi, R. (2017): “Not ‘Lone Wolves’ After All: How ISIS Guides World’s Terror Plots From Afar.” *The New York Times*, 4.2. 2017. https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html

Carter, J. A. - Maher, S. - Neuman, P. R. (2014): *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*. International Centre for the Study of Radicalisation and Political Violence. http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf

Cavana, R. Y. - Mares, E. D. (2004): “Integrating critical thinking and systems thinking: from premises to causal loops.” *System Dynamics Review,* Vol. 20, No. 3, p. 223-235. ISSN: 1099-1727

Cheong, P. H. - Gong, J. (2010): “Cyber vigilantism, transmedia collective intelligence, and civic participation.” *Chinese Journal of Communication,* Vol. 3 , No. 4, p. 471-487. ISSN: 1754-4769

Chertoff, M. – Simon, T. (2015): *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance Paper Series: no. 6. The Centre for International Governance Innovation and the Royal Institute for International Affairs. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

Choucri, Nazli et al. (2007): *Using System Dynamics to Model and Better Understand State Stability*. Working Paper CISL# 2007-03. http://web.mit.edu/smadnick/www/wp/2007-03.pdf

Cioffi-Revilla, C. (2014): *Introduction to Computational Social Science: Principles and Applications*. Springer. ISBN 978-1-4471-5661-1

Clancy, T. B. (2016a): *The Dynamics of ISIS: An Emerging-State Actor*. Worcester Polytechnic Institute. https://web.wpi.edu/Pubs/ETD/Available/etd-041416-122746/unrestricted/ISIS_Thesis_Final_4-25-16.pdf

Clancy, T. B. (2016b): “Directed, Inspired & Werther Terrorism.” *Rogue Dynamics*, 15.8. 2016. http://www.roguedynamics.com/blog/2016/8/15/op-ed-directed-inspired-werther-terrorism

Clauset, A. - Young, M. - Gleditsch, K.S. (2007): "On the Frequency of Severe Terrorist Events." *Journal of Conflict Resolution*, Vol. 51, No.1, p. 58-87, DOI: 10.1177/0022002706296157

Clauset, A. - Wiegel, F. W. (2010): “A Generalized Aggregation-Disintegration Model for the Frequency of Severe Terrorist Attacks.” *Journal of Conflict Resolution.* Vol. 54, No. 1, p. 179-197. DOI: 10.1177/0022002709352452

Clauset, A. - Woodard, R. (2013): “Estimating the historical and future probabilities of large terrorist events.” *The Annals of Applied Statistics,* Vol. 7, No. 4, p. 1838-1865. DOI:10.1214/12-AOAS614

Coleman, G. (2015): *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso. ISBN 978-1781689837

Constine, J. (2015): “ISIS Cyber Caliphate” Hacks U.S. Military Command Accounts.” *TechCrunch*, 12.1. 2015. https://techcrunch.com/2015/01/12/cyber-caliphate/

Cottee, S. (2015): “The Cyber Activists Who Want to Shut Down ISIS.” *The Atlantic*, 8.10. 2015 https://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312/

Cuthbertson, A. (2015): “Anonymous affiliate GhostSec thwarts Isis terror plots in New York and Tunisia.” *International Business Times*, 22.7. 2015. http://www.ibtimes.co.uk/anonymous-affiliate-ghostsec-thwarts-isis-terror-plots-new-york-tunisia-1512031

Cuthbertson, A. (2016): “ISIS Hackers target the Wrong Google.” *Newsweek*, 1.3. 2016. http://www.newsweek.com/isis-hackers-target-wrong-google-431911

Denning, D. (1999): "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." *Global Problem Solving Information Technology and Tools*, 10.12. 1999. http://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Denning, D. (2015): “The Rise of Hacktivism.” *Georgetown Journal of International Affairs*, 8.9. 2015. http://journal.georgetown.edu/the-rise-of-hacktivism/

Dewey, T. et al. (2012): *The Impact of Social Media on Social Unrest in the Arab Spring*. Stanford University. https://publicpolicy.stanford.edu/publications/impact-social-media-social-unrest-arab-spring

Drmola, J. (2013): “Konceptualizace kyberterorismu.” *Vojenské rozhledy*. Praha: Ministerstvo obrany České republiky, No. 2, p. 94-102. ISSN 1210-3292

Drmola, J. (2014a): “Looking for Insurgency in Cyberspace”. *Central European Journal of International and Security Studies (CEJISS)*. Prague: Metropolitan University, 2014, Vol. 8, No. 4, p. 56-77. ISSN 1802-548X

Drmola, J. (2014b): “Systémová dynamika jako nástroj pro výzkum bezpečnosti”. *Obrana a strategie*. Brno: Univerzita obrany, Vol. 14, No. 1, p. 17-30. ISSN 1214-6463

Drmola, J. - Bastl, M. - Mareš, M. (2015): “Modeling Hacktivism Using System Dynamics”. *Journal of Applied Security Research*. 2015, Vol. 10, No. 2, p. 238-248. ISSN 1936-1610

Drmola, J. (2016): „Modelling Multi-actor Security Dilemma.“ *Strategic Analysis*, Vol. 40, No. 2, p. 92-100. ISSN 0970-0161

Dutta, S. - Dutton, W. H. – Law, G. (2011): *The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online*. INSEAD. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916005

Eagle, A. (2016): “Chance versus Randomness.” *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.). https://plato.stanford.edu/archives/win2016/entries/chance-randomness/

Eikmeier, D. C. (2007): “Qutbism: An Ideology of Islamic-Fascism”. *Parameters*, Spring 2007. p. 85-97. ISSN: 0031-1723

El-Bermawy, M. M. (2016): “Your Filter Bubble is Destroying Democracy”. *The Wired*, 18.11. 2016. https://www.wired.com/2016/11/filter-bubble-destroying-democracy/

Ellis, C. et al. (2016): *Lone-Actor Terrorism*. Royal United Services Institute. ISSN 2397-0286. https://rusi.org/sites/default/files/201604_clat_final_report.pdf

Elran, M. (2017): „Societal Resilience: From Theory to Policy and Practice“. *Resilience and Risk,* p. 301-311. DOI: https://doi.org/10.1007/978-94-024-1123-2

Europol (2007-2017): *European Union Terrorism Situation and Trend Report* (TE-SAT). Europol. https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report

Europol (2016): *Internet Organised Crime Threat Assessment*. Europol. DOI: 10.2813/275589

Farmer, B. (2017): "YouTube to redirect searches for Isil videos to footage debunking their ideology." *The Telegraph*, 21.7. 2017. http://www.telegraph.co.uk/news/2017/07/21/youtube-redirect-searches-isil-videos-footage-debunking-ideology/

Farnham, N. - Liem, M. (2017): *Can a Copycat Effect be Observed in Terrorist Suicide Attacks?* International Centre for Counter-Terrorism. ISSN: 2468-0656

Fellman, P. V. - Wright, R. (2004): "Modeling Terrorist Networks, Complex Systems at the Mid-range." *The Intelligencer,* U.S. Journal of Intelligence Studies, Vol. 14, No. 2, p. 59–68. https://arxiv.org/pdf/1405.6989

Ferréol, T. B. (2016): "Hat 4Chan die russische Armee dazu gebracht, syrische Rebellen zu bombardieren?." *Motherboard*, 14.4. 2016. https://motherboard.vice.com/de/article/qkj7vd/4chan-russland-armee-syrien-rebellen-bombardieren-654

Fleming, Marie (1980): „Propaganda by the deed: Terrorism and anarchist theory in late nineteenth- century Europe". *Terrorism*, Vol. 4, No. 1, p. 1-23. http://dx.doi.org/10.1080/10576108008435483

Ford, Andrew (1999): *Modelling the Environment*. Island Press. ISBN 1-55963-601-7

Forrester, J. W. (1961): *Industrial Dynamics*. Waltham, MA: Pegasus Communications, 1999 (orig. MIT Press, 1961). 464p. ISBN 1-883823-36-6

Forrester, J. W. (1968): *Principles of Systems*. Cambridge, MA: Wright-Allen Press, 1971.

Forrester, J. W. (1969): *Urban Dynamics*. Waltham, MA: Pegasus Communications, 1999 (orig. MIT Press, 1969). 285p. ISBN 1-883823-39-0

Franceschi-Bicchierai, L. (2015): "Anonymous Has Little to Show For Its Year-Long Fight Against ISIS." *Motherboard*, 18.11. 2015. https://motherboard.vice.com/en_us/article/mg7ja3/anonymous-has-little-to-show-for-its-year-long-fight-against-isis

Gal, R. (2013): „Social Resilience in Times of Protracted Crises: An Israeli Case Study." *Armed Forces & Societ,*. Vol. 40, No. 3, p. 452-475. DOI: https://doi.org/10.1177/0095327X13477088

Gaskill, M. (2016): “Social media witch-hunts are no different to the old kind – just bigger.” *The Guardian*, 13.10. 2016. https://www.theguardian.com/commentisfree/2016/oct/13/social-media-witch-hunts

Gault, M. (2015): “The CIA Secret to Cybersecurity That No One Seems to Get.” *Wired*, 20/12/2015. https://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get/

Gilbert, D. (2016): “ISIS Twitter Hack: Meet Wauchula Ghost, Anonymous Hacker Who Defaced Islamic State Group Accounts With Gay Porn.” *International Business Times*, 20.6. 2016. http://www.ibtimes.com/isis-twitter-hack-meet-wauchula-ghost-anonymous-hacker-who-defaced-islamic-state-2384270

van Ginkel, B. - Entenmann, E. (2016): *The Foreign Fighters Phenomenon in the European Union*. International Centre for Counter-Terrorism. DOI: 10.19165/2016.1.02

Gladwell, M. (2010): “Small Change.” *The New Yorker*, 4.10. 2010. http://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell

Glazzard, A. (2017): *Losing the Plot: Narrative, Counter-Narrative and Violent Extremism*. The International Centre for Counter-Terrorism. DOI: 10.19165/2017.1.08

Greenmeier, L. (2015): “Anonymous's Cyber War with ISIS Could Compromise Terrorism Intelligence.” *Scientific American*, 19.11. 2015. https://www.scientificamerican.com/article/anonymous-s-cyber-war-with-isis-could-compromise-terrorism-intelligence/

Greenberg, A. (2017a): “Now Anyone Can Deploy Google’s Troll-Fighting AI.” *Wired,* 23.2. 2017. https://www.wired.com/2017/02/googles-troll-fighting-ai-now-belongs-world/

Greenberg, A. (2017b): „Global Police Spring A Trap On Thousands Of Dark Web Users.“ *Wired*, 20.7. 2017. https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/

Greitzer, F. L. et al. (2008): "Combating the Insider Cyber Threat." *IEEE Security & Privacy*, Vol. 6, p. 61-64, DOI:10.1109/MSP.2008.8

Hamid, S. - Dar, R. (2016): *Islamism, Salafism, and Jihadism: A primer*. The Brookings Institution. https://www.brookings.edu/blog/markaz/2016/07/15/islamism-salafism-and-jihadism-a-primer/

Hare, F. (2012): “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.” *Proceedings of the 4th International Conference on Cyber Conflict*. NATO CCD CEO. https://ccdcoe.org/cycon/2012/proceedings/d2r1s2_hare.pdf

Harris, R. (2017): *Improving our brand safety controls.* Google In Europe, 17.3. 2017. https://www.blog.google/topics/google-europe/improving-our-brand-safety-controls/

Hegghammer, T. (2016): „The Future of Jihadism in Europe: A Pessimistic View.“ *Perspectives on Terrorism,* Vol. 10, No. 6. ISSN 2334-3745.

Holmer, G. - Shtuni, A. (2017): *Returning Foreign Fighters and the Reintegration Imperative*. United States Institute of Peace. ISBN: 978-1-60127-650-6

Horgan, J. (2008): “From Profiles to Pathways and Roots to Routes.” *The ANNALS of the American Academy of Political and Social Science,* Vol. 618, No. 1, p. 80-94. ISSN: 00027162

Hosangar, K. (2016): “Blame the Echo Chamber on Facebook, But Blame Yourself Too.” *The Wired,* 25.11. 2016. https://www.wired.com/2016/11/facebook-echo-chamber/

Howard, P. N. (2011): *The Digital Origins of Dictatorship and Democracy*. Oxford University Press. ISBN 978–0–19–973641–6

Jardine, E. (2015): *Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime.* Global Commission on Internet Governance Paper Series: no. 16. Centre for International Governance Innovation and Chatham House. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2634590

Jester (2012): “Anonymous Is Getting Pwned And Not By Me.” *Jester’s Court*, 9.11. 2012. https://jesterscourt.cc/2012/11/09/anonymous-getting-pwned-and-not-by-me/

Jester (2014): “CLEAR EVIDENCE: #ISIS and other terror elements have been infiltrating Anonymous for over 2 years…” *Jester’s Court*, 29.8. 2014. https://jesterscourt.cc/2014/08/29/clear-evidence-isis-and-other-terror-have-been-infiltrating-anonymous-for-over-2-years/

Jester (2015): “How to Win a ‘Cyberwar’ with ISIS.” *Jester’s Court*, 20.11. 2015. https://jesterscourt.cc/2015/11/20/how-to-win-the-cyberwar-with-isis-a-strategy/

Jester (2017): “Russian Infiltration of the US Federal Government.” *Jester’s Court*, 28.1. 2017 https://jesterscourt.cc/2017/01/28/russian-infiltration-us-federal-government/

Johnson, N. F. – Carran S. et al. (2011): “Pattern in Escalations in Insurgent and Terrorist Activity.” *Science,* Vol. 333, p. 81-83. DOI: 10.1126/science.1205068

Johnson, N. F. – Spagat, M. et al. (2006): *Universal patterns underlying ongoing wars and terrorism*. CERAC. https://repository.royalholloway.ac.uk/file/961a47fc-1891-a6f4-0595-eb2c2725fd95/9/Sciencepaper_04-04-06.pdf

Johnston, L. (1996): “What is Vigilantism?” *British Journal of Criminology*, Vol. 36, No. 2, p. 220-236. ISSN: 1464-3529

Joscelyn, T. (2016): “Terror plots in Germany, France were ‘remote-controlled’ by Islamic State operatives.” *Long War Journal*, 24.9. 2016. http://www.longwarjournal.org/archives/2016/09/terror-plots-in-germany-france-were-remote-controlled-by-islamic-state-operatives.php

Juliano, S. (2012): “Superheroes, Bandits, and Cyber-Nerds: Exploring the History and Contemporary Development of the Vigilante.” *Journal of International Commercial Law and Technology,* Vol. 7, No. 1, p. 44-64. ISSN: 1901-8401

Karanicolas, M. - Mendel, T. (2016): *Stand Up for Digital Rights! Recommendations for Responsible Tech*. Centre for Law and Democracy. http://responsible-tech.org/wp-content/uploads/2016/06/Intermediaries-Print.pdf

Kellerman, A. (2016): *Geographic Interpretations of the Internet*. Springer International Publishing. ISBN: 978-3-319-33803-3

Kelly, S. et al. (2016): *Silencing the Messenger: Communication Apps under Pressure*. Freedom House. https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf

Kenney, M. (2010): „Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists.“ *Terrorism and Political Violence*, Vol. 22, No.2, p. 177-197. ISSN: 0954-6553

Kilcullen, D. (2017): “ISIS caliphate’s collapse will mean more terror in Europe”. *The Australian*, 26.5. 2017. http://www.theaustralian.com.au/news/inquirer/isis-caliphates-collapse-will-mean-more-terror-in-europe/news-story/cd91e67cdc15d26522f6e5f842a67fe1?nk=179dd79fa88598aed004cb93b2db81d2-1500140624

Khamis, S. - Vaughn, K. (2011): “Cyberactivism in the Egyptian Revolution.” *Arab Media and Society*, No. 13. ISSN: 1687-7721 http://www.arabmediasociety.com/articles/downloads/20110603105609_Khamis.pdf

Kimery, A. (2014): “The Jester Speaks.” *Homeland Security Today Magazine*, April/May 2014, http://www.nxtbook.com/nxtbooks/kmd/hst_20140405/index.php#/18

Kosoff, M. (2016): “ISIS Has Directly Threatened Mark Zuckerberg And Jack Dorsey.” *Vanity Fair, 25.2. 2016. http://www.vanityfair.com/news/2016/02/isis-threatens-mark-zuckerberg-and-jack-dorsey*

Kramer, F. D. et al. (2009): *Cyberpower and National Security*. Washington: National Defense University Press. ISBN: 9781597974233

Kreutzer, D. P. (1985): „A Microcomputer Workshop Exploring The Dynamics of Arms Races.“ *Proceedings of the 1985 International Conference of the System Dynamics Society*. D-3869-1, p. 463-476. http://www.systemdynamics.org/conferences/1985/proceed/kreut463.pdf

Krypt3ia (2015): *OpISIS and CharlieHebdo: Whack-A-Mole Without A Plan*. https://krypt3ia.wordpress.com/2015/02/11/opisis-and-charliehebdo-whack-a-mole-without-a-plan/

Kuypers, M. A. - Maillart, T. - Paté-Cornell, E. (2016): An Empirical Analysis of Cyber Security Incidents at a Large Organization. Workshop on the Economics of Information Security, Stanford University. https://cisac.fsi.stanford.edu/sites/default/files/kuypersweis_v7.pdf

Leweling, T. - Sieber, O. (2007): „Using Systems Dynamics to Explore Effects of Counterterrorism Policy.“ *Proceedings of the 40th Hawaii International Conference on System Sciences*. Naval Postgraduate School, Monterey. http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550198.pdf

Leyden, J. (2017): „AlphaBay and Hansa: About those dark web marketplaces takedowns.“ *The Register*, 24.7. 2017. https://www.theregister.co.uk/2017/07/24/alphabay_takedown_analysis/

Lindsay, J. R. (2015): “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack.” *Journal of Cybersecurity,* Vol. 1, No. 1, p. 53-67. DOI: 10.1093/cybsec/tyv003

Lister, C. (2016): *Returning Foreign Fighters*. The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/06/En-Fighters-Web.pdf

Magid, L. (2017): “Facebook, Microsoft, Twitter And YouTube Collaborate To Fight Terrorism.” *Forbes*, 26.6. 2017. https://www.forbes.com/sites/larrymagid/2017/06/26/facebook-microsoft-twitter-and-youtube-collaborate-to-fight-terrorism

Maillart, T. – Sornette, D. (2010): „Heavy-tailed distribution of cyber-risks.” *The European Physical Journal B*, Vol. 75, No. 3, p. 357–364. DOI: 10.1140/epjb/e2010-00120-8

Malczinsky, L. A. (2011): *Best Practices for System Dynamics Model Design and Construction with Powersim Studio.* Sandia National Laboratories, 2011-4108. http://www.systemdynamics.org/tipsfromourmembers/powersim.pdf

Manne, R. (2016): “Sayyid Qutb: Father of Salafi Jihadism, Forerunner of the Islamic State.” *ABC*, 7.12. 2016. http://www.abc.net.au/religion/articles/2016/11/07/4570251.htm

Mareš, M. (2005): *Terorismus v ČR.* Brno: Centrum strategických studií. ISBN: 80-903333-8-9

McCauley, C. - Moskalenko, S. (2008): “Mechanisms of Political Radicalization: Pathways Toward Terrorism.” *Terrorism and Political Violence*, Vol. 20 , No. 3, p. 415-433. DOI: 10.1080/09546550802073367

Meadows, D. H. (2008): *Thinking in Systems: A Primer*. Chelsea Green Publishing. ISBN: 978-1603580557

Mildeová, S. - Vojtko, V. et al. (2008*): Systémová dynamika.* Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2008. 150p . ISBN 978-80-245-1448-2

Miller, G. A. (1956): "The magical number seven, plus or minus two: Some limits on our capacity for processing information." *Psychological Review,* Vol. 63, No. 2, p. 81–97. PMID 13310704. DOI: 10.1037/h0043158

Milt, K. et al. (2017): *The European Union’s Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness*. Directorate General For Internal Policies, Policy Department C: Citizens' Rights And Constitutional Affairs, Civil Liberties, Justice And Home Affairs. http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf

Mironova, V. - Hussein, M. (2016): “The Downfall of ISIS.” *Foreign Affairs*, 26.9. 2016. https://www.foreignaffairs.com/articles/syria/2016-09-26/downfall-isis

Moreng, B. (2016): “ISIS' Virtual Puppeteers.” *Foreign Affairs*, 21.9. 2016. https://www.foreignaffairs.com/articles/2016-09-21/isis-virtual-puppeteers

Morozov, E. (2011): *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs. ISBN: 978-1-58648874-1

Mourtada, R. - Salem, F. (2011): *Civil Movements: The Impact of Facebook and Twitter*. Arab Social Media Report, Dubai School of Government. http://unpan1.un.org/intradoc/groups/public/documents/dsg/unpan050860.pdf

Moxnes, E. (2000): “Not only the tragedy of the commons: misperceptions of feedback and policies for sustainable development.” *System Dynamics Review*, Vol. 16, No. 4, p. 325–348. DOI: 10.1002/sdr.201

Murphy, L. (2015): “The Curious Case of the Jihadist Who Started out as a Hacktivist.” *Vanity Fair*, 15.12. 2015. http://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain

Nesser, P. – Stenersen, A. – Oftedal, E. (2016): „Jihadi Terrorism in Europe: The IS-Effect.“ *Perspectives on Terrorism,* Vol. 10, No. 6. ISSN 2334-3745

Neumann, P. R. (2003): “The trouble with radicalization.” *International Affairs,* Vol. 89, No.4, p. 873-893. DOI: 10.1111/1468-2346.12049

Neumann, P. R. (2013): “Options and Strategies for Countering Online Radicalization in the United States.” *Studies in Conflict & Terrorism*, Vol. 36, No. 6, p. 431-459. ISSN: 1521-0731

Neumann, P. R. (2014): „Spotting the Threat.“ *New Scientist,* Vol. 223, No. 2976, p 24-25. https://doi.org/10.1016/S0262-4079(14)61302-6

Newby, B. (2012): *Watchful Guardian or Dark Knight? The Vigilante as a Social Actor*. International Foundation for Protection Officers. http://www.ifpo.org/wp-content/uploads/2013/08/Newby_Vigilante.pdf

Newman, M. E. J. (2004): “Power laws, Pareto distributions and Zipf's law.” *Contemporary Physics*, Vol. 46, No. 5, p. 323-351. ISSN: 1366-5812

Nhan, J. - Huey, L. - Broll, R. (2017): “Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings.” *The British Journal Of Criminology*, Vol. 57, No. 2, p. 341-361. ISSN 0007-0955

Nojeim, G. T. (2010): „Cybersecurity and Freedom on the Internet." *Journal of National Security Law & Policy*, Vol. 4, p. 119-137. ISSN: 1553-3158

Norris, B. - Jempson, M. - Bygrave, L. - Thorsen, E. (2006): *Reporting Suicide Worldwide: Media Responsibilities*. http://www.mediawise.org.uk/wp-content/uploads/2011/03/Covering-Suicide-Worldwide-Updated-06.pdf

Novotný, J. - Svobodová, J. (2014): *Jak pracuje věda*. Brno: Masarykova univerzita. ISBN: 978-80-210-6942-8

OConnor, T. J. (2012): *The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare*. The SANS Institute. https://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889

Ottis, R. - Lorents, P. (2010): "Cyberspace: Definition and Implications." In *Proceedings of the 5th International Conference on Information Warfare and Security,* p. 267-270.

Pagliery, J. (2015): "Meet the vigilante who hacks jihadists." *CNN*, 16.1. 2015. http://money.cnn.com/2015/01/16/technology/security/jester-hacker-vigilante/index.html

Parkin, S. (2016): "Operation Troll ISIS: inside Anonymous' war to take down Daesh." *Wired,* 6.10. 2016. http://www.wired.co.uk/article/anonymous-war-to-undermine-daesh

Peritz, A. (2015): "Trolling ISIS." *Slate*, 19.8. 2015. http://www.slate.com/articles/news_and_politics/foreigners/2015/08/how_to_undermine_isis_with_one_simple_trick_target_the_jihadist_recruiters.html

Phillips, D. P. (1974): "The influence of suggestion on suicide: Substantive and theoretical implications of the Werther effect." *American Sociological Review,* Vol. 39, No. 3, p. 340-354. ISSN: 00031224

Polatin-Reuben, D. – Craig, R. – Spyridopoulos, T. – Tryfonas, T. (2013): „A System Dynamics Model of Cyber Conflict." *2013 IEEE International Conference on Systems, Man, and Cybernetics*. p. 303-308. DOI: 10.1109/SMC.2013.58

Pospíšil, Z. (2009): *Dynamické systémy a systémová dynamika*. Masarykova univerzita, Přírodovědecká fakulta, Ústav matematiky a statistiky. http://www.math.muni.cz/~pospisil/FILES/DynSys_SysDyn.pdf

Poznansky, M. - Perkoski, E. (2016): "Attribution and Secrecy in Cyberspace." *War on the Rocks*, 8.3. 2016. https://warontherocks.com/2016/03/attribution-and-secrecy-in-cyberspace/

Pruyt, E. - Kwakkel, J. H. (2014): "Radicalization under deep uncertainty: a multi-model exploration of activism, extremism, and terrorism." *System Dynamics Review*. Vol. 30, No. 1-2, p. 1–28. DOI: 10.1002/sdr.1510

Radzicki, M, J. - Taylor, R, A. (1997): Introduction to System Dynamics. U.S. Department of Energy, Office of Policy and International Affairs, 1997.

Quattrociochi, W. et al. (2016): „Echo Chambers: Emotional Contagion and Group Polarization on Facebook". *Scientific Reports*, Vol.6, No. 37825. DOI: 10.1038/srep37825

RAND (2017): *RAND Database of Worldwide Terrorism Incidents* (RDWTI). RAND, National Security Research Division. https://www.rand.org/nsrd/projects/terrorism-incidents.html

Reed, A. (2017): *Counter-Terrorism Strategic Communications: Back to the Future: Lessons from Past and Present*. The International Centre for Counter-Terrorism. https://icct.nl/wp-content/uploads/2017/07/FINAL-Reed-CTSC-Back-to-the-Future.pdf

Reed, A. – Pohl, J. (2017): *Tackling the Surge of Returning Foreign Fighters*. The International Centre for Counter-Terrorism. https://icct.nl/publication/tackling-the-surge-of-returning-foreign-fighters/

Reed, A. – Pohl, J. – Jegerings, M. (2017): *The Four Dimensions of the Foreign Fighter Threat: Making Sense of an Evolving Phenomenon*. The International Centre for Counter-Terrorism. https://icct.nl/publication/the-four-dimensions-of-the-foreign-fighter-threat-making-sense-of-an-evolving-phenomenon/

Reisinger, D. (2015): "Anonymous Declares Cyber War on ISIS. Why It Matters." *Fortune*, 16.11. 2015. http://fortune.com/2015/11/16/anonymous-cyber-war-isis/

Rich, E. – Martinez-Moyano, I. J. – Conrad, S. (2005): „Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model." *Proceedings of the 2005 International Conference of Sys Dynamics Society*. http://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51672.pdf

Richardson, G. P. (1991): *Feedback Thought in Social Science and System Theory*. Philadelphia: University of Pennsylvania Press. ISBN 0-8122-1332-7

Richardson, L. F. (1960): *Statistics of Deadly Quarrels*. Pittsburgh: The Boxwood Press.

Rittel, H. W. J. - Webber, M. M. (1973): "Dilemmas in a General Theory of Planning.". *Policy Sciences*, Vol 4, p.155–169. DOI: 10.1007/bf01405730

Russon, M. (2015): "Ghost Security Group: How Anonymous hackers grew up to help save the world from Isis." *International Business Times*. http://www.ibtimes.co.uk/ghost-security-group-how-anonymous-hackers-grew-help-save-world-isis-1539618

Ryan, Y. (2001): "Anonymous and the Arab uprisings." *Al Jazeera*, 19/05/2011. http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

Samuel, H. (2017): „Explosive-laden car rams police van on Paris' Champs-Elysées in botched suicide attack." *The Telegraph*, 19.6. 2017. http://www.telegraph.co.uk/news/2017/06/19/police-operation-way-champs-elysees-paris/

Scaparrotti, C. M. et al. (2013): *Cyberspace Operations*. Joint Chiefs of Staff, Armed Forces of the United States. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Schmid, A. P. (2004): "Terrorism - The Definitional Problem." *Case Western Reserve Journal of International Law*, Vol. 36, No. 2, p. 375-419. ISSN: 0008-7254

Schmid, A. P. (2011): *The Routledge Handbook of Terrorism Research*. London and New York: Routledge. ISBN: 978-0415520997

Schmid, A. P. (2017): *Public Opinion Survey Data to Measure Sympathy and Support for Islamist Terrorism: A Look at Muslim Opinions on Al Qaeda and IS*. International Centre for CounterTerrorism. DOI: 10.19165/2017.1.02

Schneier, B. (2013): „The Battle for Power on the Internet." *The Atlantic*, https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/

Schneier, B. (2015): "The Government Must Show Us the Evidence That North Korea Attacked Sony." *Time*, 5.1. 2015, http://time.com/3653625/sony-hack-obama-sanctions-north-korea/

Schneier, B. (2016): "The Value of Encryption." *The Ripon Forum*, Vol. 50, No. 2. http://www.riponsociety.org/article/the-value-of-encryption/

Schoenenberger, L. - Schenker-Wicki, A. - Beck, M. (2012): *Analysis of a Terror Network from a System Dynamics Perspective*. University of Zurich, Department of Business Administration, UZH Business Working Paper No. 322.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171240

Sedgwick, M. (2010): "The Concept of Radicalization as a Source of Confusion." *Terrorism and Political Violence,* Vol. 22, No. 4, p. 479-494. ISSN: 0954-6553

Segall, L. (2015): "The secret hackers trying to bring down ISIS." *CNN*, 20.11. 2015.
http://money.cnn.com/2015/11/20/technology/isis-ghost-security-group/index.html

Segall, L. (2016): "Meet the hacker fighting ISIS with porn." *CNN*, 16.6. 2016.
http://money.cnn.com/2016/06/16/technology/isis-hacker-porn-gay-pride/index.html

Serbu, R. – Rotariu, I. (2015): „Privacy Versus Security in the Internet Era." *Procedia Economics and Finance*, Vol. 27, p. 73-76. https://doi.org/10.1016/S2212-5671(15)00974-0

Shirkey, C. (2011): "The Political Power of Social Media". *Foreign Affairs*, Vol. 90, No. 1, p. 28–41. ISSN: 0015-7120

Silke, A. (2008): "Holy Warriors". *European Journal of Criminology*, Vol. 5, N. 1, p. 99-123. ISSN: 14773708

Singer, P. W. - Friedman, Alan (2014): *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. ISBN: 978-0199918119

Slack Alice (2017): "Facebook Fights Terrorism with AI; Is It Censorship?" *InfoSecurity Magazine,* 19.6. 2017. https://www.infosecurity-magazine.com/slackspace/facebook-fights-terrorism-with-ai/

Smallridge, J. - Wagner, P. - Crowl, J. N. (2016): "Understanding Cyber-Vigilantism: A Conceptual Framework." *Journal of Theoretical & Philosophical Criminology*, Vol. 8, No. 1, p. 57-70. ISSN 2166-8094

Smith, J. (2015): "Anonymous Divided: Inside the Two Warring Hacktivist Cells Fighting ISIS Online." *Mic*, 4.12. 2015. https://mic.com/articles/129679/anonymous-vs-isis-how-ghostsec-and-ghost-security-group-are-targeting-terrorists

Sobolewska, M. (2014): „Can we ever estimate how many British Muslims will become Islamic extremists?„ *Manchester Policy Blogs: Ethnicity*, 26.8. 2014.

http://blog.policy.manchester.ac.uk/featured/2014/08/can-we-ever-estimate-how-many-british-muslims-will-become-islamic-extremists/

Speckhard, A. (2011): *Psychosocial, Organizational and Cultural Aspects of Terrorism*. Final Report of the NATO Human Factors and Medicine Research Task Group 140. TR-HFM-140. www.dtic.mil/get-tr-doc/pdf?AD=ADA555076

Srinivasan, R. (2012): "Taking power through technology in the Arab Spring." *Al Jazeera*, 26.10. 2012. http://www.aljazeera.com/indepth/opinion/2012/09/2012919115344299848.html

START (2017): *Global Terrorism Database*. National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. https://www.start.umd.edu/gtd

Steinblatt, J. (2016): "How One 4Chan Board Is Trying To Fight ISIS In Syria." *Vocativ,* 6.6. 2016. http://www.vocativ.com/326039/how-one-4chan-board-is-trying-to-fight-isis-in-syria/

Sterman, J. D. (2000): *Business Dynamics: Systems thinking and modeling for a complex world*. McGraw Hill. ISBN 0-07-231135-5

Sullivan, K. - Wan, W. (2016): "Troubled. Quiet. Macho. Angry. The volatile life of the Orlando shooter." *Washington Port,* 17.6. 2016. https://www.washingtonpost.com/national/troubled-quiet-macho-angry-the-volatile-life-of-omar-mateen/2016/06/17/15229250-34a6-11e6-8758-d58e76e11b12_story.html?utm_term=.f084da0dfca8

Telesca, L. - Lovallo, M. (2006): "Are global terrorist attacks time-correlated?" *Physica A: Statistical Mechanics and its Applications.* Vol. 362, No. 2, p. 480-484. ISSN: 0378-4371

Toor, A. (2015): "France wants Facebook and Twitter to launch an 'offensive' against ISIS propaganda." *The Verge*, 3.12. 2015. https://www.theverge.com/2015/12/3/9842258/paris-attacks-facebook-twitter-google-isis-propaganda

Trottier, D. (2016): "Digital Vigilantism as Weaponisation of Visibility." *Philosophy & Technology,* Vol. 30, No. 1, p. 55–72. ISSN: 2210-5433

Varagur, K. (2016): "This Twitter Collective Takes On ISIS One Account At A Time." *Huffington Post*. http://www.huffingtonpost.com/krithika-varagur/this-twitter-collective-t_b_12466194.html

Vidino, L. - Marone, F. - Entemann, E. (2017): *Fear thy Neighbor*. International Centre for Counter-Terrorism. ISBN: 9788867056194.

http://www.ispionline.it/it/EBook/Rapporto_RADICALIZZAZIONE_JIHADISMO/Radicalization_web_DEF.pdf

Wade, C. (2014): "The Reddit Reckoning." *Slate*, 15.4. 2014. http://www.slate.com/articles/technology/technology/2017/07/chris_cillizza_s_reddit_ama_went_about_how_you_d_expect.html

Wilkinson, A. (2016): "We need to talk about the online radicalisation of young, white men." *The Guardian*, 15.11. 2016. https://www.theguardian.com/commentisfree/2016/nov/15/alt-right-manosphere-mainstream-politics-breitbart

Winter, C. - Clarke, C. P. (2017): "Is ISIS Breaking Apart?" *Foreign Affairs*, 31.1. 2017. https://www.foreignaffairs.com/articles/2017-01-31/isis-breaking-apart

Wolstenholme, Eric (1998): „Qualitative v. Quantitative Modelling: The Evolving Balance." *Proceedings of the 1998 International System Dynamics Conference*. http://www.systemdynamics.org/conferences/1998/PROCEED/00071.PDF

Woodall, J. (2014): "Vigilantism on the cyber frontier." *The Strategist,* 5.8. 2014, The Australian Strategic Policy Institute. https://www.aspistrategist.org.au/vigilantism-on-the-cyber-frontier/

World Bank (2017): *World Development Indicators*. World Bank DataBank. http://databank.worldbank.org/data/reports.aspx?source=world-development-indicators

York, C. (2015): "Islamic State Terrorism Is Serious But We've Faced Even Deadlier Threats In The Past." *The Huffington Post*. http://www.huffingtonpost.co.uk/2015/11/28/islamic-state-terrorism-threat_n_8670458.html

Yudkowsky, Eliezer (2008): "Cognitive biases potentially affecting judgment of global risks". In *Global catastrophic risks*, ed. Nick Bostrom and Milan M. Cirkovic, 91–119. New York: Oxford University Press. http://singularity.org/files/CognitiveBiases.pdf

Zeman, P. (2002): *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita. ISBN: 8021030372.

Zimmermann, P. R. (1999): *Why I Wrote PGP*. http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html