



JAKUB DRMOLA

**Protidžihádistický
vigilantismus
v kyberprostoru**

EDIS
Ediční řada disertačních prací
Fakulty sociálních studií Masarykovy univerzity

Svazek 18

muni
PRESS

PROTIDŽIHÁDISTICKÝ VIGILANTISMUS V KYBERPROSTORU

JAKUB DRMOLA



Masarykova univerzita
Brno 2018

Publikace byla vydána s finanční podporou Fakulty sociálních studií MU jako součást edice EDIS. Cílem edice je podpora publikačních aktivit badatelů, kteří získali titul Ph.D.

Recenzenti: doc. PhDr. Marian Brzybohatý, Ph.D.
doc. PhDr. Roman Chytilík, Ph.D.

© 2018 Jakub Drmola
© 2018 Masarykova univerzita

ISBN 978-80-210-8986-0
ISBN 978-80-210-8985-3 (brož. vaz)

PODĚKOVÁNÍ

Za odborné vedení a pomoc v průběhu celého mého studia si v první řadě zaslouží velké poděkování Miroslav Mareš. Za podněty, spolupráci, kritiku, trpělivost či plamenné akademické rozepře na půdě naší fakulty i mimo ni bych chtěl poděkovat především Romanu Chytilkovi, 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 neutu-
chající podporu během studia i mimo něj a za tolik potřebná rozptýlení,
bez nichž by průchod doktorským studiem nebyl možný.*

OBSAH

| | |
|--|----|
| 1 ÚVOD | 9 |
| 2 CÍLE | 13 |
| 3 METODOLOGIE | 15 |
| 3.1 Systémová dynamika | 15 |
| 3.1.1 Epistemologický kontext | 15 |
| 3.1.2 Historie metody | 19 |
| 3.1.3 Kauzalita a vlastnosti dynamických systémů | 20 |
| 3.1.4 Vizualizace a použití systémové dynamiky | 25 |
| 3.2 Chaos a mocninné zákony | 39 |
| 3.3 Parametry, kompromisy a vymezení modelu | 45 |
| 4 KONCEPTUALIZACE | 49 |
| 4.1 Terorismus | 49 |
| 4.1.1 Radikalizace | 51 |
| 4.1.2 Typy útoků | 53 |
| 4.2 Hacktivismus | 57 |
| 4.3 Vigilantismus | 60 |
| 4.3.1 Metody | 63 |
| 4.3.2 Aktéři | 66 |
| 4.4 Role správců digitálního obsahu | 68 |
| 5 SOUVISEJÍCÍ VÝZKUM | 70 |
| 6 REFERENČNÍ VZOREK TERORISTICKÝCH ÚTOKŮ | 73 |
| 7 MODEL PROTIDŽIHADISTICKÉHO VIGILANTISMU V KYBERPROSTORU | 80 |
| 7.1 Konceptuální a kauzální struktura | 80 |
| 7.2 Matematická a logická struktura | 86 |

| | |
|--|-----|
| 7.2.1 Demografický segment | 88 |
| 7.2.2 Radikalizační segment | 90 |
| 7.2.3 Segment generující teroristické útoky | 92 |
| 7.2.4 Segment generující oběti teroristických útoků | 96 |
| 7.2.5 Segment generující viditelnost džihadismu | 98 |
| 7.2.6 Segment soupeření v kyberprostoru | 102 |
| 7.2.7 Vigilantistický segment | 105 |
| 7.2.8 Segment svobody a bezpečnosti v kyberprostoru | 108 |
| 7.3 Výsledky simulací | 111 |
| 7.3.1 Replikace historie | 111 |
| 7.3.2 Bez eskalace řízeného terorismu | 114 |
| 7.3.3 Bez vigilantismu v kyberprostoru | 117 |
| 7.3.4 Navázání na historický vývoj | 120 |
| 7.3.5 Extrapolace vlivu vigilantismu v kyberprostoru | 123 |
| 7.4 Návrat džihadistů ze zahraničí | 126 |
| | |
| 8 ZÁVĚR | 130 |
| 8.1 Zhodnocení modelu | 130 |
| 8.2 Role vigilantismu | 132 |
| 8.3 Posouzení predikcí | 135 |
| | |
| 9 PŘÍLOHY | 140 |
| 9.1 Export rovnic modelu | 140 |
| 9.2 Odkazy ke vzorku teroristických útoků | 148 |
| 9.3 Grafické srovnání normálního rozdělení a mocinného zákona | 151 |
| 9.4 Ukázky výstupů z pseudonáhodných funkcí generujících počet teroristů podílejících se na teroristickém útoku | 151 |
| 9.5 Ukázky excesivního průběhu základní simulace | 152 |
| 9.6 Výměna mezi americkým vojákem a bojovníkem ISIS | 153 |
| | |
| 10 ZDROJE | 156 |
| | |
| 11 SUMMARY | 170 |
| | |
| 12 SEZNAM ROVNIC, TABULEK, GRAFŮ A OBRÁZKŮ | 171 |

1 ÚVOD

Tato kniha 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 hrozbu² 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

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 knihy 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 přístupováno. 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 zde nejedná o práci zabývající se analýzou hrozeb a rizik, v zájmu kompatibility a srozumitelnosti je zde užívána terminologie konzistentní s dominantním chápáním těchto pojmů v rámci české bezpečnostní komunity (viz Zeman 2002: 53–66).

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 výjimky³ 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 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. Přírozenou 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 Džihádismem⁶ motivovaná

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).

⁴ Je třeba zdůraznit, že se v žádném případě nejedná o kyberterorismus (Drmla 2013) a tato kniha 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 (*confidentiality*), celistvost dat (*integrity*) a jejich dostupnost (*availability*) (Gault 2015).

⁶ Džihádismus (Hamid – Dar 2016) je v tomto kontextu chápán jako širší, moderní hnutí, nevázané na jakoukoliv konkrétní organizaci, které násilnými

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 satirického 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, 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 útoku 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.

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>.

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).

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.

2 CÍLE

Jak vyplývá ze samotného názvu a ze situace, kterou nastínila předchozí kapitola, hlavní ambicí této knihy 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 tohoto fenoménu (pokud by se vůbec lišily). Je na místě očekávat nejen nulový (žádný vliv), ale snad i opačný, kontrainuitivní 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 model¹⁰ tedy musí být schopen zachytit džihádistický terorismus v dostatečné komplexitě a hlavně musí být schopen replikovat realitu, včetně oné významné

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 *Systémem* 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 knihy. 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 takovéhoho 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).

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 publikace 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 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 tohoto výzkumu je jako kritérium přesnosti a validity simulací stanoveno, že tyto body musí ležet v jejich 95% intervalech spolehlivosti.

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 METODOLOGIE

3.1 SYSTÉMOVÁ DYNAMIKA¹¹

3.1.1 Epistemologický kontext

Pilířem systémové dynamiky jakožto metody a vlastně i celé této knihy 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.¹²

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.¹³

¹¹ Méně podrobným a jednodušším představením této metodologie se zabýval i již vydaný článek, viz Drmola 2014b.

¹² 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.

¹³ 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

Problémem 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 se z toho vyplývajícími omezenými experimentálními možnostmi. Tato omezení plynou nejen ze zřejmých etických důvodů spojených s experimentováním na lidech, ale i z časté 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.¹⁴

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.¹⁵ Nemůžeme-li tedy experimen-

přirozené (tj. nezávislé na lidské existenci), lidské a umělé, přičemž ty umělé jsou vždy výtvozem 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 publikace je není nutné pečlivě rozlišovat (Cioffi-Revilla 2014: 7–12).

¹⁴ 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 dostatečně nízký počet zkoumaných proměnných. Bohužel zejména v oblasti bezpečnostních otázek často platí pravý opak – případů je málo a proměnných mnoho.

¹⁵ Přestože patří k těm rozšířenějším, systémová dynamika rozhodně není jedinou metodou schopnou simulovat modely komplexních sociálních systémů

tovat 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 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 konstraintivní nelinearity¹⁶ a dávají vzniknout emergentnímu

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.

¹⁶ 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 zatlumená 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