# Czech Cyber Security System from a view of System Dynamics

Ondrej Dolezal and Hana Tomaskova*

*Faculty of Informatics and Management, University of Hradec Kralove,*
*Rokitanskeho 62, Hradec Kralove, Czech Republic*
*E-mail: ondrej.dolezal@uhk.cz; hana.tomaskova@uhk.cz*
**Corresponding Author*

Received 06 August 2018; Accepted 31 October 2018;
Publication 19 November 2018

## Abstract

With the rapid development of information and communication technologies and the increasing dependence of modern civilization on them, the number and significance of threats to the functioning of the whole of society (not only smart society) are constantly increasing. Prevention, security, and protection against cyber threats pose a challenge that will have to be faced in the future. This article presents systems thinking and system dynamics approaches to solving complex problems and shows their potential use in cybersecurity, with a particular focus on the current state of cybersecurity in the Czech Republic.

**Keywords:** Cybersecurity, System dynamics, system thinking, Czech Republic.

## 1 Introduction

Cybercrime is a complex and ever-changing phenomenon but the major problem is the absence of a consistent current definition, even among those law enforcement agencies charged with tackling it [47]. For example, Wall [46] states that “cybercrimes are crimes that are mediated (governed) by networked technology and not just a computer”.

*Journal of Cyber Security and Mobility, Vol. 8_2,* 241–260. *River Publishers*
doi: 10.13052/jcsm2245-1439.824
*This is an Open Access publication.* © 2018 *the Author(s). All rights reserved.*

The Police of the Czech Republic [36] define cybercrime as a crime that is “committed in an environment of information and communication technologies where the subject of the attack is either the area of information and communication technologies itself or the crime is carried out with a significant use of information and communication technologies”.

The National Cyber and Information Security Authority (NUKIB) [31], which is the central administrative authority for cybersecurity, including the protection of classified information in information and communication systems, and also cryptographic protection in the Czech Republic, defines cybercrime as: “Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity”.

According to the National Cyber Security Strategy (NSKB) [33], the possibilities of trading sensitive information is growing. The character of the Internet gives offenders the opportunity to perform both targeted and massive attacks, and promises quick action and profit, while at the same time low risk of punishment. The report of the Ministry of the Interior [28] identifies an increase in information criminality. All forms of crime have been growing fastest for many years in the Czech Republic and the rest of the world, and a change in the role of the Information and Communication Technologies (ICT) cannot be expected.

Unfortunately, there is an extremely high latency rate in this area, as evidenced by the [1, 21], and most cases remain undetected or unreported. The total number of incidents, automated and targeted attacks, both successful and unsuccessful, estimated the Ministry of the Interior in 2014 to approximately 200,000 incidents per day. The European Union Agency for Network and Information Security (ENISA) [12] points out that the trend in 2016 has been monetising cybercrime, attacks are becoming more sophisticated and optimized for profit. The European Union (EU) in the investigated materials [9, 44] comprehensively addressed cybersecurity, in addition to such concrete steps. In the legislation, but rather generally, they addressed cooperation between security forces and organisations, industry, science and academia, business opportunities and roofing, and support for co-operation of all components at national and interstate level.

The development of cybercrime techniques is growing rapidly, the professionalisation of criminals of information criminality, which is increasingly sophisticated with a clearer division of individual roles, the perpetrators are increasingly trying to mask their behavior using cryptographic mechanisms, often also using botnets that contribute to anonymity, massiveness and technological coordination of the attack. At present, not all EU countries have the necessary means and capabilities to fight cybercrime effectively [9]. Europol [14] states that cybercrime annually costs EU countries 256 billion euros, and worldwide 900 billion euros.

### 1.1 System Dynamics and Modeling

The system approach is based on the fact that the system cannot be understood by reducing to smaller units but by accepting the complexity of connecting all parts and their arrangement which is non-reducible [6]. According to Capra [5], "understanding things by systemically means literally putting them in context, determining the nature of their relationships" and systemic thinking means "understanding phenomena in the context of a larger entity", which is also related to the original meaning of the term system.

System dynamics is a science that investigates the behavior of systems over time. System dynamics, according to Forrester [16], is an essential foundation for effective system thinking. According to Richmond [37], systemic thinking is the basis for system dynamics. System Dynamics offers a set of tools to understand the structure and behavior of complex systems. It is a practically oriented discipline that helps to better understand the surrounding systems, especially those in which there is a high degree of detailed and dynamic complexity [4, 41]. According to Forrester [18], models should be compiled from all available information, including mental models and both written and numerical information, with only a tiny part of the available information. The result of the analysis (simulation) of the finished model should be to improve mental models.

For the purpose of this article, Stella 10.0 software is used to model systems. This program is a work of iSee systems (originally High Performance Systems), founded in 1985 by Barry Richmond [7].

## 2 Cyber Threats

The Oxford Dictionary [11] defines cyber threat as "The possibility of a malicious attempt to damage or disrupt a computer network or system".

## 2.1 Types of Cyber Threats

For now, perhaps the most comprehensive overview of cyber threats can be found in ENISA's annual publication—the ENISA Threat Landscape Report 2017 [13]. ENISA also publishes threat overviews for specific areas such as smart grid, IoT, smart hospitals, and so on. In this publication, the threats are divided into 15 top cyber threats, as listed below:

- Malware,
- Web-based attacks,
- Web application attacks,
- Phishing,
- Spam 45,
- Denial of service,
- Ransomware,
- Botnets,
- Insider threat,
- Physical manipulation/damage/theft/loss,
- Data Breaches,
- Identity theft,
- Information leakage,
- Exploit kits,
- Cyber-espionage.

## 2.2 Cybernetic Threats for the Czech Republic

In the Czech Republic, several organisations dealing with Cyber Security, for example:

- The National Office for Cybernetics and Information Security [32] (NUKIB),
- The National Center for Cyber Security [30] (NBU),
- The Committee on Cyber Security [45] (VKB),
- The Department of Cyber Security and Coordination of Information and Communication Technologies of the Ministry of Interior [27].

Legislation within the Czech Republic (Act No. 240/2000 Coll., on Crisis Management and on Amendments to Certain Acts (Crisis Act) and Government Decree No. 432/2010 Coll., Criteria for Determining Critical Infrastructure Element as amended by Amendment No. 315/2014 Coll.) defines Critical Information Infrastructure (KII) and Significant Information

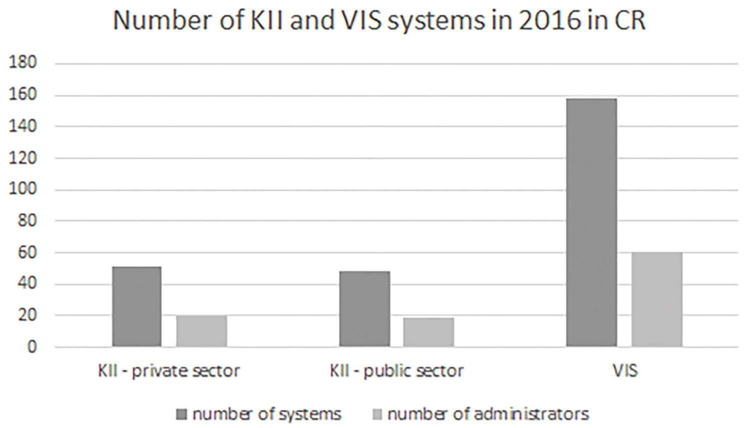

**Figure 1** Number of KII and VIS systems in 2016 in CR [20].

Systems (VIS) and becomes an obligation for their operators and administrators. The system is categorised by the NBU in co-operation with stakeholders. Figure 1 shows the latest available data.

The National Cyber Security Strategy for the Year 2015–2020 [33] (NSKB) poses many more general and specific threats. More common threats include: mobile malware, large data and cloud (for its non-transparency), social networking, switching from IPv4 to IPv6, embedding and exploiting backdoor hardware. More specific threats to the Czech Republic were identified in the NSKB:

- CR as a possible test facility: = The Czech Republic uses similar technologies, mechanisms and processes as other states to protect itself, and threatens to serve attackers to test attacks on more prominent states. Against the threat of attacks and fighting in cyberspace, Balaban, Pernica and coll. [1] also warn and warn against disinformation campaigns to influence public opinion, which are the current conflicts.
- Insufficient public trust in the state: = Security will not work without the co-operation of all citizens, the private sector (most cyberspace [33]) and cyber-security organisations.
- Threats associated with digitisation of public administration (eGovernment).
- Protection of industrial control systems and information systems in healthcare.

- Increasing dependence of defense components on ICT Systems, networks and technology itself (vehicles, aircraft, ...) are endangered, which threatens the defense of the state and the conduct of military actions. Defensive components must be able to respond to cyberthreats and disable them.
- Low Digital Literacy of End Users Basic awareness of potential threats is missing from public and government users.
- Threats related to the Internet of Things (IoT) and Intelligent Power Networks (Smart Grid) = The digitisation of formerly passive systems brings new opportunities for abuse, the number of devices connected to the Internet is constantly increasing and their security is often miserable, as the Ministry of the Interior points out. This is compounded by the illiteracy of users.
- Lack of cybersecurity experts and the need to revise existing curricula in education.
- Insufficient security for small and medium-sized businesses.
- Increasing numbers of Internet users and ICTs and the resulting criticism of their failure.
- Increasing cybercrime and cyber attacks.

## 3 System Approach to Cybersecurity

Savage and Schneider [39] explain that security cannot be scaled by adding hardware or software but that it is the property of the whole system arising from the relationships between its elements. This explains why cybersecurity requires a strategy that is based on a system approach. This strategy then requires organisations to adopt security technologies and understand the risks.

Given that the need for a comprehensive and sophisticated approach to cybersecurity is relatively new, there is not much to mention about the benefits that come from the system access application.

At Massachusetts Institute of Technology (MIT), the cradles of system approach, among other things, deal with incident evaluation [38] and a Systems-Theoretic Accident Model and Processes (STAMP) based on a system approach was developed to evaluate security incidents and risks, as well as to design methodologies for their prevention and methodologies for their evaluation. STAMP works with system constraints and boundaries, control loops, process models, and control levels. It also looks at the fact that systems are socio-technical, meaning that a human factor that influences the process directly and physically, but indirectly through different rules and regulations, plays a significant role. STAMP has been applied to examples of security and aeronautical security events, and the possibility of its use in cybersecurity has been introduced using the CAST (Causal Analysis Based on STAMP) method, which was used to analyze incidents and their causes.

In 2015, a Cyber Attack Impact Assessment (CAIA) methodology was introduced to assess the impact of a cybercrime attack on critical infrastructure. CAIA similar to STAMP, respectively CAST, including a human factor. The methodology CAIA compares behavior without incidents and incident incidents, examines control variables, observed variables, and events occurring in processes. The possibilities of using the methodology ranging from risk assessment to network design control were highlighted and the possibility that the methodology could also use attackers to prepare for a more devastating attack was also highlighted.

## 4 Model of the Cyber Security System of the Czech Republic

A causal-loop diagram was selected to represent the system. Only core elements, loops, and relationships are shown. The system interacts with the environment and is therefore open. We can label this system as dynamic because it evolves over time. Furthermore, the system can be classified as hierarchical because it can be divided into smaller soft and hard subsystems.

Outside the system, but with a strong influence on it, there are elements, such as: the geopolitical situation of the state, natural and other influences and the lobby.

The following elements of the system are used in the causal Figure 2:

- Lobby – The impact on media, legislation and finance is considered.
- Finance – The amount of funds needed to ensure the functioning of security organisations and educational and scientific activities. Availability of finance can be positively influenced by the awareness of cybersecurity populations and threats.
- Legislation and other rules – Includes laws, decrees, but also rules and internal rules and policy of organisations (not only security but all private and public entities, profit and non-profit).
- Security Organisation – Includes organisations and other cybersecurity units. Their interdependence and co-operation can be modeled as a standalone subsystem and all available data suggests it is of good quality.

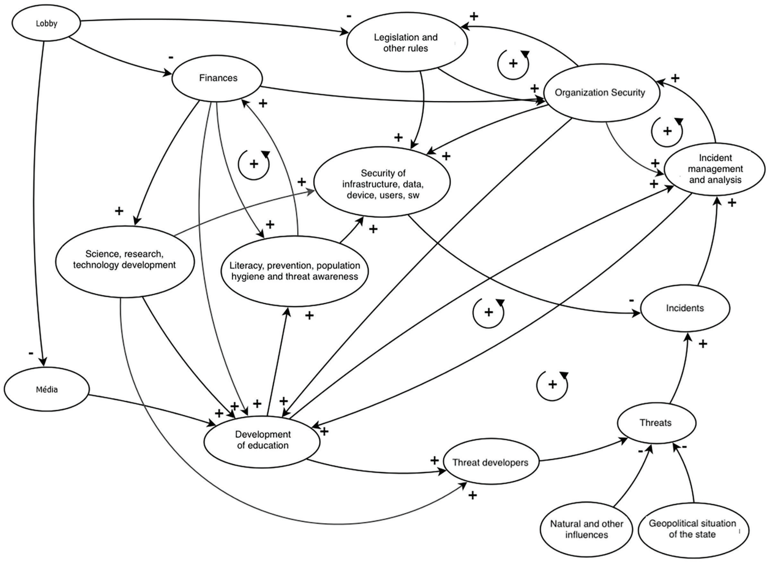
Lobby
Legislation and other rules
Finances
Organization Security
Security of infrastructure, data, device, users, sw
Incident management and analysis
Science, research, technology development
Literacy, prevention, population hygiene and threat awareness
Incidents
Média
Development of education
Threats
Threat developers
Natural and other influences
Geopolitical situation of the state

**Figure 2** CR cybernetic security system.

*Source:* own processing by [35].

- Incident Management – Includes the collection of data on incidents (including cybercrime) and their analysis, which ideally provides information on the origin of threats and includes a proactive, real-time and reactive approach
- Science, Research, Technology Development – Includes activities in the field of science and research. They contribute to security development and also to threats.
- Security of Infrastructure, Devices, Software, Data, Users – This element consists of two levels of subsystems where security should be the property of each.
- Literacy, prevention and hygiene of the population – This is the result of educational and awareness-raising activities. An enlightened population contributes to infrastructure, equipment and data security.
- Incidents – Includes all security incidents and cybercrime crimes.
- Media – Includes print, radio, cinema, television, the internet and other media through which education and awareness can be disseminated. Currently, the Czech Republic is primarily used for the dissemination of professional information for security specialists but there are good examples of television and radio.

- Development of education – Represents all educational and educational activities, including education in schools. It is therefore a summary of training, courses, exercises and trainings, teaching materials and human capacities. At present, most activities are primarily targeted at network administrators and other IT specialists.
- Threat Developers – Includes threat makers and available information about them. Developing technology and education will also have a positive impact on their skills and professionalisation and role-sharing.
- Threats – Includes all kinds of threats. Threat developers have an impact on them, and specific threats are becoming incidents.
- Natural and other influences – Heavy-handed elements that should not be omitted.
- Geopolitical Situation of the State – Affects threats and threats

### 4.1 System Dynamics Model of the Cyber Security System of the Czech Republic

Both the Eurostat and the Czech Statistical Office (CZSO) provide a broad spectrum of very basic statistics on the Internet connection of individuals and households, connected devices, the use of eGovernment, e-commerce, the share of IT staff in total employment, and so on. Unfortunately, more comprehensive statistics on cyber threats are missing or are very general and often contain only data for the years 2010 and 2015. The CZSO investigated threats and security only in the mentioned years on the initiative of Eurostat.

The Czech police publish cybercrime statistics as of 2011, in Figure 3, including the distribution of the most frequent groups of crimes. However, all detected values are subject to high latency.

Individual threat statistics are generally published by companies operating in the field of computer security but they often only concern the networks they manage or the threats their anti-virus software reveals.

For the dynamic model shown in the Figure 6, the development of the number of cybercrime crimes has been chosen. The total number of incidents depends on several variables, of which the main ones can be calculated quite accurately, others cannot yet be quantified. Although threat analysis has shown that many types of threats are independent on the Internet, much more is associated with the Internet and increasing risk will increase. Both individuals and businesses using the Internet are the richest ones unsecured. Therefore, the development of the number of affiliated enterprises and individuals, including their security, was included in the model.

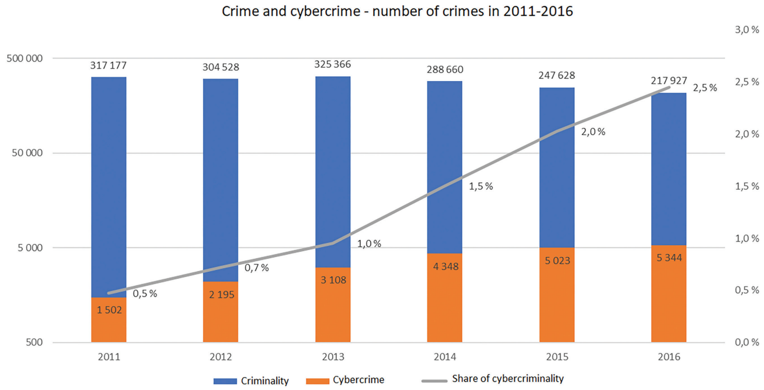

**Figure 3** Dynamic model of cybercrime.

*Source:* own processing.

After multiplying by the proportion of unsecured users, the enterprises get the number of the most vulnerable devices, suitable for attack, their total numbers can be expressed by relations:

$$P_u = (U_t.U_c).U_d,$$

$$P_c = (C_t.C_c).C_d,$$

where $U_t$ represents the level of vulnerable users, $U_c$ represents the rate of connected users, $U_d$ represents user devices and $C_t$ represents the level of vulnerable companies, $C_c$ represents the rate of connected companies, $C_d$ represents company devices.

The annual influx of crimes can be described by the equation:

$$y = (a.P_u) + (b.P_c) + (c.P_x),$$

where the regression was determined by the members k and q, representing the weights of the individual variables and the member$(c.P_x)$ which can be interpreted as other causes of cybercrime is at present mathematically indescribable.

The statistics of cybercrime have been published by the Czech Police since 2011, this year was therefore chosen as the beginning of the simulation. The simulation is conducted from 2017 for another 5 years. Due to the rapid development of ICT, longer-term forecasts cannot be made.

The sub-parts of the model from the Figure 6 are:

- The proportion of users – which expresses the development of the number of individuals using the Internet, according to CZSO data processed in Figure 4.

- The proportion of business – which expresses the share of businesses connected to the Internet. Although the large enterprise connection rate is approaching 100%, small businesses are lagging behind, and they are newly connected and unsecured (or their devices) may be the target of attack. The average share of all enterprises was determined on the basis of CZSO data as weighted average of individual enterprises by their size, where the weights are the frequencies of the enterprises in the given group, data processed in Figure 5,

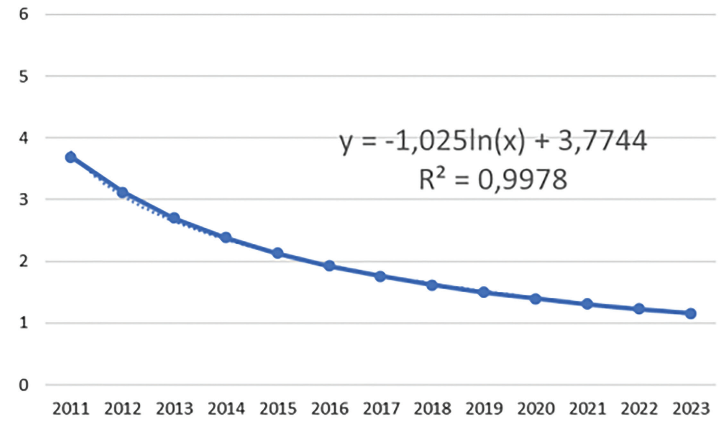

**Figure 4** Increase in internet users in the Czech Republic, own processing.

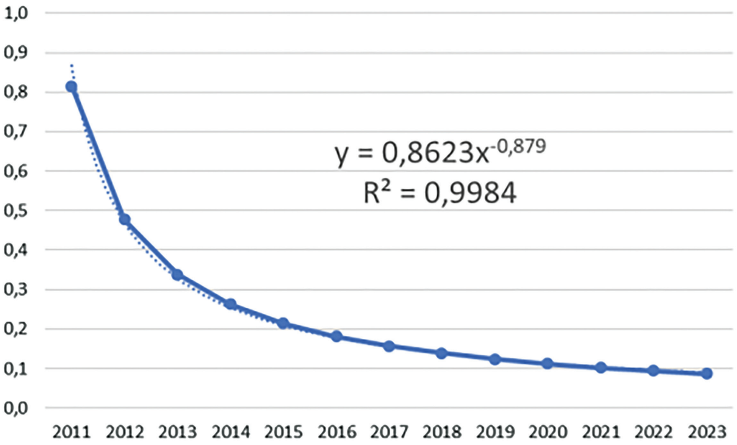

**Figure 5** Increase of businesses with the Internet in the Czech Republic, own processing.

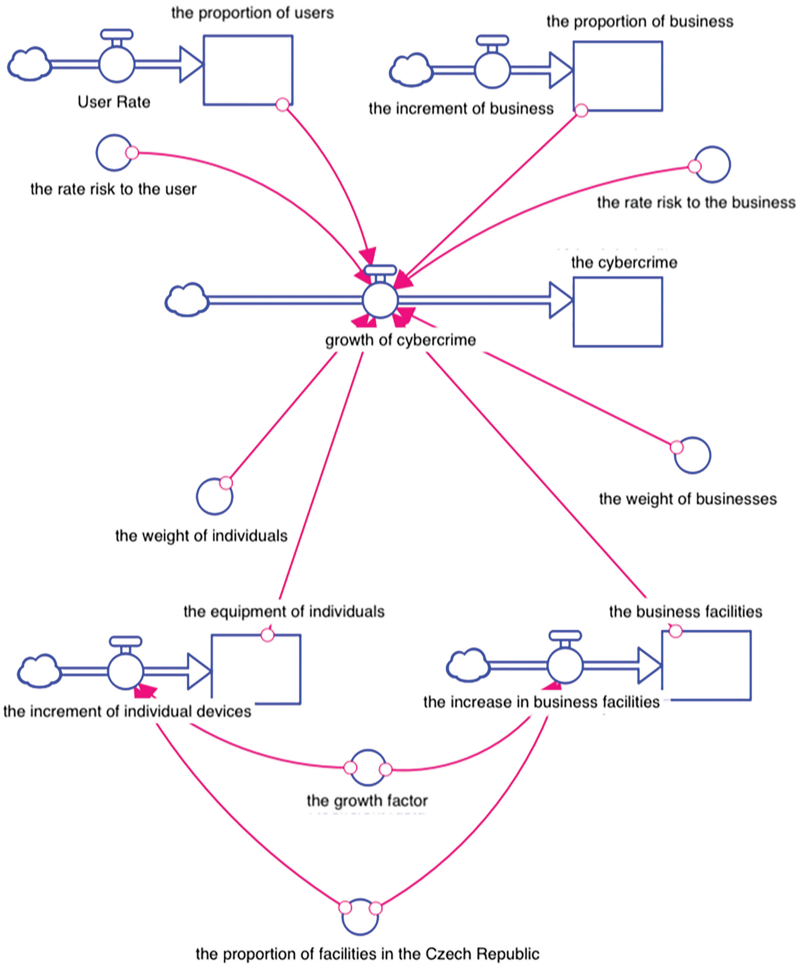
the proportion of users
User Rate
the proportion of business
the increment of business
the rate risk to the user
the rate risk to the business
the cybercrime
growth of cybercrime
the weight of businesses
the weight of individuals
the equipment of individuals
the business facilities
the increment of individual devices
the increase in business facilities
the growth factor
the proportion of facilities in the Czech Republic

**Figure 6** Dynamic model of cybercrime, own processing.

- The rate risk to the businesses – coefficient is based on the only available data, according to the CZSO survey of 2016 [34], according to which 20.5% of enterprises do not address data security and are therefore among the most vulnerable.
- The rate risk to the user – the coefficient is established according to the only available data of the CZSO from 2010, when it was found that 23% of users did not know how their computers were secured, which can be interpreted as lacking in the overview of cyber threats and the basic level of digital literacy and their devices are most at risk.

- The cybercrime – the total number of crimes of cyber crime since the beginning of the simulation.
- Growth of cybercrime – the annual number of cybercrime crimes.
- The equipment of individual and business facilities – which represents the number of devices connected to the Internet used by individuals/ businesses in millions of pieces. The features used describe the number for the whole world multiplied by the share of equipment in the Czech Republic, while the ratio of enterprise facilities and individuals remains the same. The evolution of the quantity is based on data from Gartner [26], which implies an exponential growth in the total number of installations from 3.9 billion in 2014 to over 6.4 billion in 2016 to 20.8 billion in 2020.
- The proportion of facilities in the Czech Republic – which is a coefficient expressing part of the total number of devices in the world that belong to the Czech Republic. This is based on the number of establishments per 1 inhabitant of the Czech Republic. Symantec, using Gartner's predictions, said that in the US, 0.25 devices were available per inhabitant in 2016, according to statistics from statista.com [40], which was 2.9 devices per person in 2014. The same source states for Germany a value of 2.4. By default, the number of devices per inhabitant of the Czech Republic (with a greater emphasis on Symantec's compatibility with Gartner data) was approximated to 0.5 per person in 2011, according to the CZSO population data.
- The growth factor – which allows you to control increment of device count during simulation. At default value 1, it has no effect.

## 5 Simulations

The results of the simulation in the default setting correspond to the statistics of the Police of the Czech Republic for the past years. Because of latency mentioned in the discussion and due to the temporary incalculability of other sub-causes of cybercrime, it is not possible to reduce data abstraction and simulate more accurate outputs. The model is ready for future refinement of some elements based on newly available or discovered facts.

Simulated data are reported in the Tables 1 and 2 where

- A = The increase in business facilities,
- B = The business facilities,
- C = The increment of individual devices,
- D = The equipment of individuals,
- E = The cybercrimes.

**Table 1** Simulation results in the default setting

| Years | A | B | C | D | E |
|---|---|---|---|---|---|
| 2011 | 0.28 | 0.94 | 0.45 | 1.31 | 2009.49 |
| 2012 | 0.37 | 1.22 | 0.61 | 1.76 | 2390.19 |
| 2013 | 0.48 | 1.59 | 0.82 | 2.37 | 2893.48 |
| 2014 | 0.63 | 2.08 | 1.11 | 3.19 | 3560.76 |
| 2015 | 0.82 | 2.71 | 1.49 | 4.30 | 4446.44 |
| 2016 | 1.07 | 3.52 | 2.01 | 5.79 | 5622.61 |
| 2017 | 1.39 | 4.59 | 2.71 | 7.80 | 7185.07 |
| 2018 | 1.81 | 5.98 | 3.64 | 10.51 | 9261.16 |
| 2019 | 2.36 | 7.79 | 4.91 | 14.15 | 12020.20 |
| 2020 | 3.07 | 10.15 | 6.61 | 19.06 | 15687.4 |
| 2021 | 4.00 | 13.22 | 8.9 | 25.67 | 20562.3 |
| 2022 | 5.21 | 17.22 | 11.99 | 34.57 | 27043.42 |

**Table 2** Simulation results with slower device development and decreasing threat level

| Years | A | B | C | D | E |
|---|---|---|---|---|---|
| 2011 | 0.28 | 0.94 | 0.45 | 1.31 | 2010.07 |
| 2012 | 0.37 | 1.22 | 0.61 | 1.76 | 2391.01 |
| 2013 | 0.48 | 1.59 | 0.82 | 2.37 | 2906.16 |
| 2014 | 0.63 | 2.08 | 1.11 | 3.19 | 3578.51 |
| 2015 | 0.82 | 2.71 | 1.49 | 4.30 | 4471.13 |
| 2016 | 1.03 | 3.52 | 1.94 | 5.79 | 5563.52 |
| 2017 | 0.80 | 4.55 | 1.55 | 7.73 | 6361.95 |
| 2018 | 0.86 | 5.35 | 1.73 | 9.28 | 6920.59 |
| 2019 | 0.94 | 6.21 | 1.96 | 11.01 | 7171.21 |
| 2020 | 1.08 | 7.15 | 2.33 | 12.97 | 7618.57 |
| 2021 | 1.25 | 8.23 | 2.79 | 15.3 | 7944.68 |
| 2022 | 1.52 | 9.49 | 3.49 | 18.09 | 8301.7 |

The main cybercrime trends are shown in Figure 7 for both strategies.

The outputs of the first simulation are shown in Table 1 and Figure 7, which assumes that all elements are in the basic setting; i.e., from 2016 a sharp increase in the number of devices.

The outputs of the second simulation are shown in Table 2 and Figure 7, which is a slower evolution of equipment in future years and also takes into account the evolution of the threat rate of individuals and businesses over time, and the gradual development of educational activities and population development. An overall improvement of 10% was achieved in the final year of the simulation.

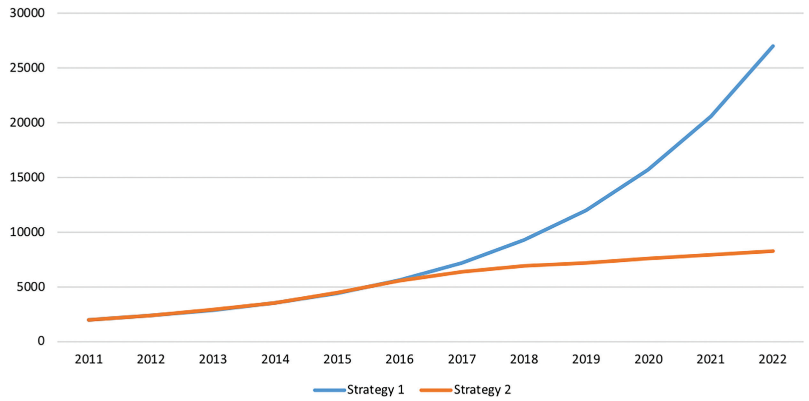

**Figure 7** Development of cybercrime, for two strategies, own processing.

## 6 Discussion

The research of cybercrime models is predominantly focused on the economic aspect of the problem. A systematic investigation in Belgium that queried the costs and impact of cybercrime was presented in [19], network economic model of cybercrime with a focus on financial services was presented in [29]. The author in [3] adapted the cost model of cybercrime by examining data regarding costs and losses inflicted by cybercrime. Another area of cybercrime research is mainly devoted to the detection of cybercrime [23, 24] or network models using game theory [2].

System dynamics is mostly used to look at things globally and not very simplistically, for example [4, 8, 10, 15, 16, 17, 18, 22, 37, 41, 42, 43].

Understanding systems through structure and behavior transferability offers the ability to compare cybersecurity with other similar systems. Cybersecurity has to be seen as an evolutionary system, so it is a comparison with public health. The well-described property that emerges at system level is, for example, group immunity. If the population is predominant in health and vaccinated individuals, then illnesses will spread worse, which also provides protection to weaker, healthier or unvaccinated persons [25].

There is currently not enough relevant and complete data for a detailed quantitative description of cyber threats and security. In the case of incident analysis, the role of continuous methodology is assessment, and the financial and other impacts of incidents are so far only estimates. Individual threat statistics are generally published by companies operating in the area of computer security and they often only concern the networks that they manage or the threats that their anti-virus software reveals.

This model is limited by the short period from which the input data originates. The model would be considerably more profitable if there were enough data to examine each group of companies by size because SMEs are the most vulnerable. If the development of computer security awareness and literacy within the CR population is broken down by age group, then the most vulnerable groups could be studied—that is, children and seniors.

## 7 Conclusion

An analysis of cybercrime from the point of view of systemic dynamics has shown that the current approach is able to exploit the exemplary cooperation of all interested organisations at the level of the Czech Republic and the EU.

A dynamic simulation of the cybercrime model has helped to outline future developments and has shown that, if the predicted growth forecasts of the number of devices are met, then there will be a large increase in the number of offences. On the contrary, assuming the development of awareness and moderate growth, the simulation showed that the development of the number of crimes would be milder and more manageable.

## Acknowledgments

The authors would like to thank to our student, A. Ostruszka , for cooperation on topic. The support of SPEV FIM UHK is kindly acknowledged.

## References

[1] Balaban, M., and Pernica, B., et al. (2015). *Security system of the Czech Republic: problems and challenges*. Charles University in Prague, Karolinum Press.

[2] Bartholomae, F. (2018). Cybercrime and cloud computing. a game theoretic network model. *Managerial and Decision Economics*, 39(3), 297–305.

[3] Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Varstvoslovje: Journal of Criminal Justice & Security*, 16(2).

[4] Bures, V. (2011). *System Thinking for Managers*. Professional Publishing.

[5] Capra, F. (2004). Tissue of life, new synthesis of mind and matter. Technical report, ISBN 80-200-1169-2.

[6] Chen, H. T. (2016). Interfacing theories of program with theories of evaluation for advancing evaluation practice: Reductionism, systems thinking, and pragmatic synthesis. *Evaluation and Program Planning*, 59, 109–118.

[7] Chichakly, T., Our story.

[8] Cimler, R., Tomaskova, H., Kuhnova, J., Dolezal, O., Pscheidl, P., and Kuca, K. (2018). Numeric, agent-based or system dynamics model? which modeling approach is the best for vast population simulation? *Current Alzheimer Research*, 15(8), 789–797.

[9] European Commission. Cybersecurity strategy of the european union: An open, safe and secure cyberspace, Feb 2013.

[10] De Savigny, D., and Taghreed, A. (2009). *Systems Thinking for Health Systems Strengthening*. World Health Organization.

[11] Oxford Dictionaries. (2018). cyberthreat — definition of cyberthreat in us english by oxford dictionaries.

[12] ENISA. Enisa threat landscape report 2016, Feb 2017.

[13] ENISA. Enisa threat landscape 2017, Jan 2018.

[14] Europol. European cybercrime centre - ec3, 2017.

[15] Forrester, J. W. (1995). The beginning of system dynamics. *McKinsey Quarterly*, pages 4–17.

[16] Forrester, J. W. (1999). System dynamics: The foundation under systems thinking. *Sloan School of Management. Massachusetts Institute of Technology*.

[17] Forrester, J. W. (2007). System dynamics the next fifty years. *System Dynamics Review*, 23(2-3), 359–370.

[18] Forrester, J. W. (2009). Some basic concepts in system dynamics. *Sloan School of Management–MIT*.

[19] Holt, T. J., Brewer, R., and Goldsmith, A. (2018). Digital drift and the sense of injustice: Counter-productive policing of youth cybercrime. *Deviant Behavior*, pages 1–13.

[20] Holy, R. (2017). Report on cyber security of the Czech Republic 2016.

[21] Kolouch, J. (2016). *Cybercrime*. CZ.NIC, 2016.

[22] Maresova, P., Tomaskova, H., and Kuca, K. (2016). The use of simulation modelling in the analysis of the economic aspects of diseases in old age. In *Business Challenges in the Changing Economic Landscape-Vol. 1*, pages 369–377. Springer.

[23] Mbaziira, A., and Jones, J. (2016). A text-based deception detection model for cybercrime. In *Int. Conf. Technol. Manag*.

[24] Mbaziira, A., and Murphy, D. R. (2018). An empirical study on detecting deception and cybercrime using artificial neural networks. In *Proceedings of the 2nd International Conference on Compute and Data Analysis*, pages 42–46. ACM.

[25] Jessica E Metcalf, C., Ferrari, M., Graham, A. L., and Grenfell B. T. (2015). Understanding herd immunity. *Trends in immunology*, 36(12), 753–755.

[26] Meulen, R. Gartner says 6.4 billion connected.

[27] MVCR. Department of cyber security and coordination of information and communication technologies.

[28] MVCR. Situation report on selected areas of safety 2014, Mar 2015.

[29] Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, 7(1), 70–81.

[30] NBU. Introduction, 2018.

[31] NUKIB. Cyber security glossary. *The National Cyber and Information Security Authority*, 2015.

[32] NUKIB. Introduction, 2015.

[33] NUKIB. National cyber security strategy of the Czech Republic 2015–2020, Feb 2015.

[34] Czech Statistical Office. Information society in figures - 2016, 2016.

[35] Ostruszka, A. (2017). Threats from the point of view of system thinking.

[36] PCR. Cybercriminity.

[37] Richmond, B. (1994). System dynamics/systems thinking: Let's just get on with it. In *International systems dynamics conference, Sterling, Scotland*.

[38] Salim, H. M. (2014). *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks*. PhD thesis, Massachusetts Institute of Technology.

[39] Savage, S. and Schneider, F. B. (2009). Security is not a commodity: The road forward for cybersecurity research. *Retrieved May*, 31, 2010.

[40] Statista.com. Number of connected devices per person in selected countries 2014 — statistics.

[41] Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Irwin/McGraw-Hill.

[42] Tomaskova, H., Kuhnova, J., Cimler, R., Dolezal, O., and Kuca, K. (2016). Prediction of population with alzheimers disease in the european union using a system dynamics model. *Neuropsychiatric disease and treatment*, 12, 1589.

[43] Tomaskova, H., Kuhnova, J., and Kuca, K. (2016). Ageing and alzheimer disease-system dynamics model prediction. *Ceska a Slovenska farmacie: casopis Ceske farmaceuticke spolecnosti a Slovenske farmaceuticke spolecnosti*, 65(3), 99–103.

[44] Shared Vision. Common action: A stronger europe. a global strategy for the european unions foreign and security policy. URL: http://www.eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf, 2016.

[45] VKB. Introduction, 2018.

[46] Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, volume 4. Polity.

[47] Yar, M. (2013). *Cybercrime and Society*. Sage.

## Biographies

**Ondrej Dolezal**, is a young researcher (PhD student supervised by HT). His focus is on mathematical modeling, computer science, computer simulation (Agent Based Modeling, system dynamic) and object modeling (UML, BPMN).

**Hana Tomaskova,** Ph.D. published more than 90 works: Including four papers published in impacted paper (one other is in the press and 4 others are under review in journals) 40 papers are listed in database of web of science, 29 papers are listed in Scopus database.

HT is an author of one book and a coauthor of another book. During her doctoral studies, she specialised in marketing and optimisation in special algebras. As a postdoc, she has also begun to focus on modeling, namely System Dynamics, Agent-Based Modeling, UML and, most recently, BPM, which allows her to use everything from her previous studies. Citations 60, H-index WOS 5.