AARMS Vol. 16, No. 1 (2017) 5–16.

Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program[1]

László KOVÁCS,[2] András NEMESLAKI,[3] Ákos ORBÓK,[4] András SZABÓ[5]

Information communication technology (ICT) has changed our life and it has a determinant role in our everyday activities; over the last years it has created a constantly changing, developing and complex ecosystem. In this paper, we argue, that this newly formed environment, requires new approaches for exploring technology and society relationships, and we pose the general question how pervasive ICT ecosystem shape interactions and relationships between humans and technology on different levels. This question is pivotal for understanding challenges of information security; in our contribution, we present a four-phase comprehensive research program systematically analysing a) our new smart environment, b) various dimensions of information security awareness, c) the role of leadership and finally d) the importance of strategic alignment.

Keywords: *information, communication, technology, security, research*

Introduction

Moore's law which is the driving force of exponential progress in technology performance has enabled computers and computing to become an everyday social experience by embedding connected microchips into everyday artefacts, basically surrounding us by smart objects. This new paradigm of computing involves digitally mediated embodied experiences in everyday activities through everyday artefacts where the interface between material and human has disappeared. [1] As, however, ICT has become ubiquitous and affordable, pressure on innovation has also become more widely spread. In a fascinating monograph, former Google CEO Eric Schmidt and Jared Cohen, a foreign relations and counterterrorist expert, paint an exciting new world of the future in the digital age—how ICT reshapes people, businesses and nations all together. [2]

As argued, not only economical competitiveness and our national security is determined by information communication technologies (ICT), but we can safely say that almost all our social interactions and everyday practices have become intertwined with technology. In the case of these exponentially developing ICT tools and services the basic question arises; does

1 The work was created as a commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled "Public Service Development Establishing Good Governance" in the Ludovika Workshop.

2 Professor of National University of Public Science; e-mail: kovacs.laszlo@uni-nke.hu
3 Professor of National University of Public Science; e-mail: nemeslaki.andras@uni-nke.hu
4 Assistant professor of National University of Public Science; e-mail: orbok.akos@uni-nke.hu
5 Assistant professor of National University of Public Science; e-mail: szabo.andras@uni-nke.hu

this fast-paced development also mean that our vulnerability and dependency is increasing? Are we becoming more exposed to risks by using this new infrastructure? New innovative tools, systems and services appear in our everyday life with such a high-level of complexity that ordinary users can hardly, if at all, orient themselves in this new socio-technical ecosystem.

The symbiosis of technology and society is most dominant in urban settings, since half of the globe lives in this habitat. [3] Even more, according to UN statistics, in 2012, already 78% of population of the developed countries was living in cities, but due to demographic, environmental and economic reasons migration to urban areas is a major trend in the developing world as well. [4] Technology plays and should continue to play a major role in contributing to the quality of life, support sustainability and simply provide innovative solutions to manage the living conditions in these more and more overcrowded urban spaces.

So far regulation of cyberspace, strategies to tackle the vulnerabilities, and policies to address security have been treated on a national states' level—according to traditional strategy making paradigms. [5] After looking at several attempts in European countries, analysing their relevant documents and decrees, it is apparent that some countries take a general approach, considering this problem an overarching challenge of an information society, and some others, intend to tackle it as a specific concern of security addressing it from a critical infrastructure point of view. [6]

The general question in our research program is how the pervasive ICT ecosystem shapes user behaviour, what type of opportunities and threats arise in this environment, and how strategic thinking can mitigate risks and seize opportunities in this new era of human-technology relationship. In this essay, we outline the epistemological foundations of this issue and propose a research agenda to systematically address the above challenges; concretely, we provide a framework on how institutional level cyber strategies can be developed in the pervasive computing era, or—looking at the other side of this coin—investigating how emergent behavioural challenges can be translated to higher level strategies ensuring a safely working ICT based ecosystem.

Theoretical Foundations

We anchor our research approach of cyber security to the dialogues of science technology studies[6] (STS), [7] due to the interdisciplinary nature and topical fitting to the discourses about how technology shapes social institutions and how social institutions—such as governments—influence technology development and adoption.

Advocates of STS argue that there is no such thing as a social problem that does not have technological components; nor can there be a technological problem that does not have social components, and so any attempt to make such a division is bound to fail. They suggest that the development of technological devices should be interpreted within an analysis of the struggles and growth of "systems", having components both human and technological, or "networks" consisting of entities, concepts, artefacts, humans and—very importantly—complex relationships between them. [8] This approach to the study of technology uses the "seamless web" or "actor-network" metaphors, [9] which stress the importance of paying attention to the different but interlocking elements of physical artifacts, institutions and their environments, blurring different levels of analysis. [10]

6 Some sources use the phrase Science-Technology-Society under the same acronym, basically referring to the same broad church of scholarship. For instance, [11] has this approach.

In order to develop a framework in STS, within which operational research design can be implemented, we took two explanatory theories for defining our research constructs.

The first of these set of theories are the offspring of Anthony Giddens's structuration theory, specifically its application in information systems. [12] [13] In the centre of structuration concepts we find structure: which is defined as a set of rules and resources organized as properties of social systems. Systems, furthermore, are reproduced relations between actors or collectives, organized as regular social practices. Social structure is constantly created through the flow of everyday practices, shaped by a mutually constitutive duality of agency and institutions. As Orlikowski has shown, this constitutive duality can be extended to the human-technology relationship where none of the two are in preference to the other—there is simply an inseparable interplay between emergent technology driven user behaviour and institutionally constraining strategies and regulations. [14] Emergent behaviour is formulated through mechanisms which are ways things happen due to the interactions of actors. Constructs of emergency, for instance, can be described using Actor-Network Theory, [9] which inherently treats technology and human actors symmetrical. Stabile working structures emerge as a mechanism of human-machine interplay where flexible routines influence flexible technologies. Leonardi describes this alteration of technology and routine interactions as "imbrication of agencies" where for instance new technology is constrained by old routines or new routines generate new features of technology. [15] Material agency influences emergent behaviour by its feature set and it is both constraining and enabling at the same time. Symmetrically, human agency can also be constrained by several features of institutional, cultural, biological limitations or path-dependencies.

The second theoretical foundation of our research program originates from general strategic management, and its classic application in information management focusing on the so called "fit" and "alignment". [16] Alignment addresses both how ICT is aligned with the business and how the business should or could be aligned with ICT. When discussing business-ICT alignment, terms such as "harmony", "linkage", "fusion", "match" and "integration" are frequently used synonymously with the term alignment. Alignment is about the process to ensure that the organizational strategies adapt harmoniously both horizontally and vertically.

Alignment of IT strategy with the organization's business strategy is a fundamental principle advocated for over 25 years, [17] it also has been an evergreen dilemma on the top list of information management issues both for senior IT managers and business executives. [18] Educating line management about the possibilities and limitations of information technology is very hard, as is setting IT priorities for projects, developing resources and skills, and generally integrating systems with strategy. It is even tougher to keep business and IT aligned, as business strategies and technologies evolve. Economic shifts caused by events such as innovative entrepreneurial ideas, regulatory changes, new innovations or international security scandals bring in dramatic swings as how to respond.

There is a strong evidence in the information management literature that IT has the power to change industries and markets. [19] [20] This very broad stream of research also shows that adoption of IT driven innovation, moreover economic returns of IT investments only happen when it is coupled with organizational change, [21] process redesign, [16] systemic skill development of employees and high level management commitment at conception and execution in tandem with professional project management at implementation. [22] Alignment, on the other hand, gets much less attention in relation to the public IT domain, while

the importance of value delivery in e-governance has been heavily emphasized. [23] We argue, that strategic alignment models (SAM) serve as useful frameworks in public administration—for instance with regards to cybersecurity strategies as well—as they do in a business setting.

Alignment processes—coupled with the concepts of social construction of technology—are the glue holding together previous decisions or external dependencies of IT suppliers, contacts with other governments or elements of the ICT ecosystems which determine the risks of our new virtual world in cyberspace.

Research Model for Information Security Strategy Construction

On the previously outlined theoretical foundations we developed a research design and complex program to investigate how information security strategies are formulated and constructed. As we argued in the previous section, our interest focuses on two general theories as foundations—the social construction of human-technology structures and the alignment coupled with ICT and organizational fit processes. In the complex ecosystems of technology, institutions, regulations, legislations and organizations, these processes move top-down (strategy execution – institutional approach) and bottom-up (behavioural emergency – agency approach). When we designed our research model, depicted in Figure 1, we hypothesized that these are non-exclusive flows (right and left arrows) and they work in tandem, constructing a special dynamic of maturity shaping both the strategy process and the environment we live in.

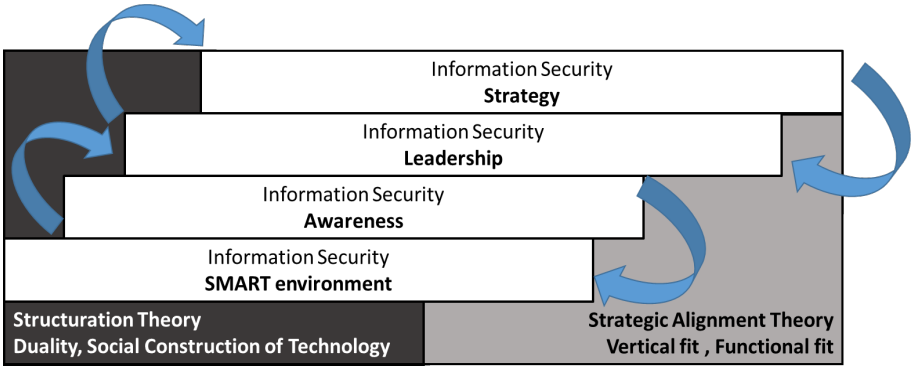

Figure 1. Research Model for Information Security Strategy Process.
(Edited by the authors.)

In Figure 1 we depicted four key constructs of this idea, which need to be tested and verified according to a robust research design and complex program. In this section, we describe the key elements of this design and the rational of including them into the research model. These are in the order shown in Figure 1 and are Information Security (IS) issues in our smart city environments, IS awareness living and working in this environment, how leadership reacts and influences behaviour and, finally based on all this, how IS strategy institutions are created and operate.

Analysing the Duality of Advanced Technology and Society Relationship in the Urban Environment

As we have argued, the most significant habitat of the future human-technology ecosystem will be urban areas in all parts of the world. There are two main conceptual beliefs pressing against each other in this setting which, in our opinion, require thorough investigation. The first is the effectiveness and efficiency orientation encouraging and seeking out ICT innovations, new business models and setting directions in city improvements such as transportation, energy utilization, public safety, and pervasive services such as health monitoring. The second, is a deep sociological and human orientation emphasizing the threat to privacy, individual control over one's decisions, the disappearance of local communities, and a lifestyle when virtual reality will dominate human connections.

With our contribution in this chapter we intend to explore this dichotomy and to explore its mechanisms with the following:

- identifying the risk factors which threaten the "smart city" concept both from an ICT infrastructural point of view and from a human and social point of view;
- categorizing approaches in smart cites according to challenges in infrastructure management, public safety, law enforcement, and privacy management;
- observing and experimenting with everyday human-computer interaction in urban setting, like traveling, communicating, and using services, and seeking out patterns of behaviour and new social norms;
- analysing the interactions of stakeholders and mapping how the social-business-technology ecosystem is structured within which smart cities operate;
- documenting new norms of equipment use, effectiveness of intelligent and pervasive services, and the new roles of regulatory institutions.

During our research program, we would like to test the main hypothesis of this chapter, that is by disassembling the complex social and technology structures into elementary pieces we can improve our understanding of the structuration process within the complex network of institutions, human actors, ICT components, social norms, innovative services, and higher level security and safety.

Behavioural Analysis in Cyberspace: Assessment of Information Security Awareness

In the pervasive computing environment, non-intentional use of technology is natural, and with the disappearance of digital divide in organizations and societies motivational and economical barriers are not significant any more. Therefore, in this phase we focus on intentional use, that is, awareness in order to explore critical challenges of user behaviour, especially from a security perspective. As anecdotal experience and lots of research shows, documented requirements and campaigns have little impact on changing attitudes [24] [25] and behaviour in this context, therefore a deep understanding of information security awareness is essential for understanding human-computer interaction in the future.

To analyse the user behaviour and awareness we will use experimental design, focused group sessions and unique exercises and scenario building borrowed and adopted from military experiences. The following topics will be explored here:

- understanding how users handle anonymity and digital presence in different environments;
- understanding how organizations manage their cyber assets and regulatory interfaces for controlling individual use;
- modelling the complexity of defence organisms, mapping the complex relationships of human actions, policies, technology and different stakeholders;
- creating scenario based demonstrations to help recognize cyber security for users to make cyber incidents understandable and visual for them;
- creating cyber security Table Top Exercise (TTX) scenarios, and a platform to easily perform such policy level exercises (using collaboration, data visualization and scenario management tools);
- analysing security exercises like Cyber 9/12, Locked Shields, CDX, and several others, we create recommendations for organizations on how to enhance organizational learning with simulations.

Education and learning are key drivers for increasing awareness. In this respect, efficiency of ones individual learning process highly depends on ones capabilities, motivation and most importantly the learning methods. Acquiring previously unknown skills and latest knowledge is always easier if the learner is interested in the topic. Nowadays, cyber skills are not only "good to have", but have become a "must have" skill in nearly all fields and professions. So, it is very important to highlight these skills in a university curriculum, and also to create teaching materials which are easy to learn, while keeping students´ interested. [26] A novel approach to increase cyber security awareness is the gamification of the education. [27] While years earlier security awareness training was characterized as a dark classroom full of people watching an annual presentation about the importance of IT security, nowadays these are much better envisioned by using online materials, demonstration videos and being engaged in interactive exercises. In our research, we are looking for more sophisticated methods to support future needs of skill development, like attack simulations, educational games and role play. We are looking for such methods to increase the efficiency of the learning process, to ease the workload of instructors, and to make education an enjoyable experience.

Talent management is also important to prepare cyber security experts for their future jobs, to keep them in the profession and to track their professional development. [28]

Our main hypothesis in this chapter is that such complex human-technology relationships can only be successfully tested and explored if a proper environment is available where actions-reactions can be simulated and practical experience can be gained.

Analysing Changes in Strategic Thinking and Leadership in Cyberspace

Strategic thinking and leadership approaches are traditionally top-down and driven by a clear hierarchy of objectives. Mission statements and objectives are set at high level and, institutionally, they are broken down to goals, action items, programs and projects. This paradigm is characterized by a strong deterministic view, expected lower levels abide by the higher ones. Managerial mind-set therefore revolves around phrases such as, alignment, compliance, fit, and classic feedback mechanisms. [29]

In the course of this research chapter we intend to explore how the phenomena of technology driven emergency influences traditional top-down strategic thinking by investigating the following areas:

- Describing emergent behaviour in the era of pervasive computing. Emergent behaviour is formulated through mechanisms, which are ways how things happen due to the interactions of actors. [30] Alteration of technology and routine interactions for instance can be described as imbrication of agencies where new technology is constrained by old routines or new routines generate new features of technology.
- Studying emergency with the use of Actor-Network Theory [9] which inherently treats technology and human actors symmetrical. Stabile working structures emerge therefore as a mechanism of human-machine interplay where flexible routines influence flexible technologies.
- Running focused group sessions with information security executives to explore the counter pressing forces between institutional alignment to high-level objectives and emergent behaviour as a result of employee-technology structuration.
- Analysing cases of successful and unsuccessful leadership attempts to create organizational alignment, and apply action research principles for seeking out solutions through ongoing consultations with information security managers, policy makers and experts.

Once we have a better understanding of emergency and, importantly, its interpretation by managers, leaders and policy makers we intend to formulate how traditional technology deterministic strategic thinking can be improved by the inclusion of emergency.

Strategic Approaches for Information Security: Mechanisms of IT Alignment

As experience shows, strategic documents, which address policy issues, leadership actions and desired regulatory responses have serious deficiencies in taking into consideration the dynamism in technology innovations especially in ICT. [6] The wide gap between these plans and the rate of change in ICT development results in delayed government responses, disorientation amongst economic actors, and quite often misinterpretation of broader social implications of technology adoption. We intended to address the conceptual problem that existing strategies and plans are, therefore, insufficient for achieving sustainable results in high level public policies. This challenge, furthermore, results in inappropriate regulations, inadequate legislations leaving many of the technology´s pressing social implications unanswered. [31]

In this research chapter, we plan to execute the following experiments:

- analysis of the existing international strategies, white papers and policy documents analysing cyberspace;
- analysis and evaluation of the Hungarian (national) documents addressing the same issues;
- juxtaposition of technology—especially ICT—state of the art and rate of change with strategic initiatives in these documents, showing how this juxtaposition impacts public administration, economic policy and national security;
- explore how the dialogue between different actors, leadership, and institutions structure social practices, which later on get documented and codified;
- based on these findings and the research results of chapters 1–3 create a conceptual model on how technology induced change in leadership, security awareness and everyday social practices can be incorporated in strategic planning, programs and legislative initiatives.

Based on these results we would like to prove our hypothesis that successful strategic planning and documentation of information security policies require taking into consideration the change of ICT development, and the complex intertwining of technology-society dynamism.

As a summary, our general assumptions, or testable research questions for our program, can be outlined as follows:

- Information security assessment in contemporary pervasive ICT environment can only be assessed through situated actions, observing and analysing human-technology interaction, during real use.
- ICT penetration in urban habitats has a measurable impact on social behaviour creating effectiveness and efficiency in several areas, but creating tremendous challenge in areas of privacy and security.
- Incorporating the concept of emergency into strategic thinking improves organizational alignment and enables better technology adoption. When managers, leaders and policy makers understanding is widened with emergent thinking, they are more likely to find strategic solutions which create adherence to information security principles.
- The dynamics of ICT is a determining factor for creating policy level information security documents. Without analysing and incorporating the transformative power of ICT into the policy setting information security strategies are likely to fail.

Research Methodology and Expected Contributions

As far as methodology is concerned in the field of STS a wide range of conceptual tools and techniques are accepted for the investigation of the construction of socio-technical entities. [32] It is important to have in mind, however, that this approach rejects both technological and social determinism: it thus goes beyond traditional approaches that are concerned with assessing the "impacts" of technology, in order to examine what shape the technology has these "impacts" and the way in which these impacts are achieved. [10] Therefore we plan to apply a set of methodologies which are not only suitable to test our hypotheses but are also in alignment with duality and the relational ontology of human and material. The key methodologies we are going to use are experimental design, comparative policy analysis, and action research.

Experimental Design:
For the analysis of Research Chapter 1–3 experimental design is planned as key methodology. We set up both controlled simulations using the ICT research environment, and anthropological observations on how users behave in situated actions. [33] The variety of ICT equipment, the situations, and the scenarios, combined with the selection of participants will provide the empirical basis of testing hypotheses in these research chapters. Naturally, experiments will be combined with broader data gathering, as we might explore such constructs, which need different verification. [34] We will also apply focused group sessions and log analysis in order to enrich our data and information about human-machine interaction.

Comparative Policy Analysis:
Both our theoretical framework and the concrete needs of Research Chapter 4 require the institutional analysis of technology society relationship. In our case this will entail policy

analysis and text mining of strategy documents. Using this set of methodologies rich narratives of interviews, case study collections and systematic comparison of different information security and cyber defence strategies will be developed. [35] Transcripts of the expert workshops will also be included, and other secondary data sources will be juxtaposed to the empirical findings throughout the document analysis.

Action Research:
Action research aims to solve current practical problems while expanding scientific knowledge. Unlike other research methods, where the researcher seeks to study social phenomena but not to change them, action research is concerned with solving particular problems and simultaneously studying the process. It is strongly oriented toward collaboration and change involving both researchers and subjects. [36] We will use this methodology with information security managers to capitalize on learning both by the researchers and these managers within the context of their social system. By doing so, we create a clinical method, similar to a consultation process which puts researchers in a *helping role* with practitioners. Using the laboratory as a clinical setting we will diagnose situations both for the managers and for the researchers creating a collaborative learning environment. Using theories and models in the learning process we will induce collaborative change. In this therapeutical stage, we will study the effects and impacts of this change.

The human-technology experiments will be executed in a computer laboratory setting.

As far as contributions are concerned we expect the following key achievement as our program unfolds:

a) An English language monograph containing the results of the four Research Chapters published at a recognized and prestigious publisher.
b) Theoretical foundations of the problem statement, its relevance and the significance of anchoring our empirical work to Science Technology Studies will be published as peer reviewed scientific working paper, open for access to a wide audience at an early stage of our research.
c) Empirical results and hypothesis testing of Research Chapters 1. to 4. will be published in peer reviewed, prestigious and/or ranked international or Hungarian journals (four journal papers).
d) At the end of the first year a focused workshop will be organized by inviting Hungarian and international experts in order to ensure the relevance of the research design and the empirical experimentations during the following two years. The workshop is also expected to provide visibility and anchoring of the program both domestically and internationally.
e) Detailed research experiments, results and their analysis will be presented during the first two years of the program; all in all, 4 peer reviewed scientific conference presentations (two in each year) will be delivered and published in proceedings.
f) By the end of the program two new Ph.D. research topics will be developed, accompanied by necessary course components.
g) At the end of the third year, we organize a conference for both high level decision makers and academic professionals as a summit of the research program and as a forum to present the key findings.

Conclusions

In our paper, we presented a comprehensive research program—its theoretical foundations, research design, methodology and expected contributions in the field of information security.

We argued, that justification of this program is underlined by empirical results, and the dynamics of IT development suggest in the public domain the complex relationship between technology and society has to be taken into consideration. Information systems are not composed of technology alone, they are systems which emerge from the mutually transformational interactions between the information technology and the organization. The duality of this relationship is essential for understanding how innovation is enabled by ICT, because information systems are as much the result of ICT enabling an organization, as much as an organization enables an information system. Furthermore, both the economic value and the broader social value of such systems depend on how successfully this duality works, and how ICTs and organizations create new institutionalized socio-technical systems.

Therefore, the socio-technical systems approach is crucial for investigating the interrelatedness of technological and social systems. By drawing attention to the intertwining and interpenetration among technological and human processes, the socio-technical systems approach serves, and rightfully so, as a major policy making framework for ICT strategies and achieving better alignment.

We presented two foundational theories: Giddens structuration theory and Henderson Venkatraman's IT strategic alignment modelling. Based on these foundations we constructed a four-phase IS strategy formulation process—with top-down and bottom-up directions.

These four constructs concluded in four main research questions or complex testable hypotheses focusing on structuration in smart technology environments, security awareness of individuals in complex ecosystems, influences of human-technology duality on leadership and management; and finally, the high-level strategy formulation and alignment of institutions satisfying the bottom-up emergencies and top-down execution requirements.

We believe that the early stage publication of our initiative is relevant both for academia and practice, since our main objective with this paper—and with the whole research program—is to generate discussions between as many participants of the new cyber ecosystem as possible.

REFERENCES

[1] YOO, Y.: Computing in everyday life: A call for experiental computing. *MIS Quarterly,* 34 2 (2010), 213–231.

[2] SCHMIDT, E., COHEN, J.: *The New Digital Age: Reshaping the Future of People, Nations and Business.* New York: Alfred A. Knopf, 2013.

[3] MEIJER, A., BOLÍVAR, M.: Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences,* 82 2 (2016), 392–408.

[4] UNITED NATIONS, D. o.: *World Urbanization Prospects: The 2014 Revision.* ST/ESA/SER.A/366. 2015.

[5] CHOUCRI, N., MADNICK, S., FERWERDA, J.: Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, 20 2 (2014), 96–121.
[6] KOVÁCS L.: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. *Hadmérnök*, 7 2 (2012), 302–311.
[7] HACKETT, E., AMSTERDAMSKA, O., LYNCH, M., WAJCMAN, J.: *The Handbook of Science Technology Studies.* (3. ed.) Cambridge: MIT Press, 2008.
[8] MERALI, Y.: Complexitiy and Information Systems. In. MINGERS, J., WILLCOCKS, L. (Eds.), *Social Theory and Philosophy for Information Systems.* 407–446. Chichester: John Wiley & Sons, 2004.
[9] LATOUR, B.: *Reassambling the social: An introduction to actor-network theory.* Oxford, UK: University Press, 2005.
[10] HOWCROFT, D., MITEV, N., WILSON, M.: What We May Learn from the Social Shaping of Technology Approach. In. MINGERS, J. WILLCOCKS, L. (Eds.), *Social Theory and Philosophy for Information Systems.* 329–371. Chichester: John Wiley & Sons, 2004.
[11] SZEKELY I.: Building Our Future Glass Homes: An Essay About Influencing the Future Through Regulation. *Computer Law and Security Review*, 29 8 (2013), 540–553.
[12] JONES, M., ORLIKOWSKI, W., MUNIR, K.: Structuration Theory and Information Systems: A Critical Reappraisal. In. MINGERS, J. WILLCOCKS, L. (Eds.), *Social Theory and Philosophy for Information Systems.* 297–328. Chichester: John Wiley & Sons, 2004.
[13] JONES, M. R., KARSTEN, H.: Giddens's structuration theory and information system research. *MIS Quarterly*, 32 1 (2008), 127–157.
[14] ORLIKOWSKI, W.: The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, 3 3 (1992), 398–427.
[15] LEONARDI, P. M.: When flexible routines meet flexible technologies: affordance, constraint and the imbrication of human and material agencies. *MIS Quarterly*, 35 1 (2011), 147–167.
[16] VENKATRAMAN, N.: IT-enabled business transformation: From automation to business scope redefinition. *Sloan Management Review*, 35 2 (1994), 72–87.
[17] HENDERSON, J. C., VENKATRAMAN, N.: Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, 32 1 (1993), 472–484.
[18] LUFTMAN, J.: *Competing in the Information Age.* New York: Oxford University Press, 2003.
[19] PORTER, M. E.: Strategy and the Internet. *Harvard Business Review*, 3 (2001), 63–78.
[20] BRYNJOLFSSON, E., SAUNDERS, A.: *Wired for Innovation: How Information Technology is Reshaping the Economy.* Cambridge: MIT Press, 2010.
[21] MANYIKA, J., NEVENS, M.: Technology after the bubble. *McKinsey Quarterly*, Special Edition (2002), 17–27.
[22] BANNISTER, F., REMENYI, D.: The Societal Value of ICT: First Steps Towards an Evaluation Framework. *Electronic Journal of Information Systems Evaluation*, 6 2 (2003), 197–206.
[23] BANNISTER, F., CONNOLLY, R.: Forward to the past: Lessons for the future of e-government from the story so far. *Information Polity*, 17 3–4 (2012), 211–226.
[24] BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly*, 34 3 (2010), 523–548.

[25] ILLÉSSY M., NEMESLAKI A., SOM Z.: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom*, 14 1 (2014), 52–73.
[26] SWARAT, S.: What Makes a Topic Interesting? A Conceptual and Methodological Exploration of the Underlying Dimensions of Topic Interest. *Electronic Journal of Science Education*, 1 (2008).
[27] BOOPATHI, K. S.: Learning Cyber Security Through Gamification. *Indian Journal of Science and Technology*, (2015), 624–649.
[28] BUTTYÁN L., FÉLEGYHÁZI M., PÉK G.: *Mentoring talent in IT security: A case study.* www.usenix.org/system/files/conference/ase16/ase16-paper-buttyan.pdf (Downloaded: 14 3 2017)
[29] BALATON K., HORTOVÁNYI L., INCZE E., LACZKÓ M., SZABÓ Z. R., TARI E.: *Stratégiai menedzsment.* Budapest: Aula Kiadó, 2010.
[30] CECEZ-KECMANOVIC, D., GALLIERS, R. D., HENFRIDSSON, O., NEWELL, S., VIDGEN, R.: The Sociomateriality of Information Systems: Current Status, Future Directions. *MIS Quarterly*, 38 3 (2014), 809–830.
[31] BELÁZ A., BERZSENYI D.: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. *Stratégiai Védelmi Kutatóközpont Elemzések*, 3 (2017), 1–15.
[32] LEE, A.: Thinking about Social Theory and Philosophy for Information Systems. In. MINGERS, J., WILLCOCKS, L. (Eds.), *Social Theory and Philosophy for Information Systems*. 1–26. Chichester: John Wiley & Sons, 2004.
[33] SUCHMAN, L.: Feminist SST and the Sciences of the Artificial. In. HACKETT, E. AMSTERDAMSKA, O., LYNCH, M., WAJCMAN, J. (Eds.), *The handbook of science and technology studies*. 139–164. Cambridge: MIT Press, 2008.
[34] HINE, C.: *Virtual Methods: Issues in Social Research on the Internet.* Oxford, New-York: Berg, Reprint, 2008.
[35] CAULIER-GRICE, J., DAVIES, A., PATRICK, R., NORMAN, W.: *The theoretical, empirical and policy foundations for building social innovation in Europe (TEPSIE).* Brussels: European Commission: 7th Framework Programme DG Research, 2012.
[36] BASKERVILLE, R., MYERS, M.: Special Issue on Action Research in Information Systems: Making IS research relevant to practice. *MIS Quarterly*, 28 3 (2004), 329–335.