# The Balanced Digitalization and Digital Security: Case of Regional Authorities

**Tuija Kuusisto[1, 2] and Rauno Kuusisto[1, 3, 4]**
**[1]Ministry of Finance and National Defence University, Helsinki, Finland**
**[2]University of Jyväskylä, Finland**
**[3]The Finnish Defence Research Agency, Riihimäki, Finland**
**[4]National Defence University, Helsinki, Finland**
tuija.kuusisto@vm.fi
rauno.kuusisto@mil.fi

**Abstract:** The emerging digital infrastructure enables the public authorities to shape their processes and to create attractive digital services for the citizens and the business actors. The public processes, services and infrastructure, however, engage with global and local public and private digital infrastructure and service providers. The complex comprehensiveness of the digital infrastructure and the services challenges the public authorities and create new types of security risks. The achieving of the benefits of the digitalization of public processes and services without increasing security risks requires the adopting of novel approaches to digital security. The paper refers to a framework that aims to balance the digitalization and digital security of society. The approach follows the complex adaptive system and social system theories. The paper demonstrates the framework with widely known digital service indexes and digital security indexes. The paper applies the referred framework and the results of its demonstration in a case study about the governing of the digitalization resources and activities of the regional authorities. The case study was related to a major structural reform. The aim of the reform was to form and launch the operations of new counties. The means of the reform included the co-creation of new types of digital processes and services in collaboration and with the citizens and the business actors as well as with the central government. The empirical data of the case study included the ICT costs, digitalization efforts, shared ICT services and digital security situation of the regions. The central government analyzed the empirical data for the simulation of the financial negotiations between the central government and the regions. The results of the case study show that the framework supported the outlining of the contents of the empirical data so that both the digitalization and digital security aspects were concerned and visualized. The authorities will apply the results of the analysis for the governing of the regions.

**Keywords:** complex systems, modelling of digital security, cyber security, system modelling, digital services, regions

## 1. Introduction

The emerging digital infrastructure enables the public authorities to create attractive digital services for the citizens and the business actors. The infrastructure, including IoT devices and autonomous systems, provides splendid opportunities to the authorities to improve the public processes and services. Merriam-Webster (2019) gives a traditional definition of digitalization as 'The process of converting something to digital form'. Gartner's (2019) statement of digitalization follows a broadly accepted modern view as it defines digitalization as 'The use of digital technologies to change a business model and provide new revenue and value-producing opportunities'. Recently the public sector authorities have increasingly considered this modern view. They have applied information and communication technology and information management and analysis for shaping the public processes and services. The authorities have usually attempted to enhance the citizen and the business actor experience of the services in addition to reducing the public sector total costs. The digitalization efforts have often included the creation of new digital processes, services and infrastructure. This has required continuous change management of the civil servants, citizens and the business actors as well as processes and technology.

The public processes, services and infrastructure engage with global and local public and private digital infrastructure and service providers. The complex comprehensiveness of the digital infrastructure and the services challenges the public authorities and creates new types of security risks. Digital security is an emerging term referring to the security view on digitalization and digital services. Typically, it includes information and cyber security and data protection. Often it covers risk management, and preparedness and contingency planning as well. The achieving of the benefits of the digitalization of public processes and services without increasing security risks requires the adopting of novel approaches to digital security.

First, the paper refers to a framework that aims to balance the digitalization and digital security of society (Kuusisto & Kuusisto, 2017). The approach follows the complex adaptive system (Holland, 1996) and social system theories (Parsons, 1951), (Habermas, 1984 & 1989). The approach adopts a social system model that aim

is to increase understanding about the evolving features and culture of the digital era (Kuusisto, 2004). The paper demonstrates the framework with widely known digital service indexes and digital security indexes.

The indexes contain indicators for measuring information society (ITU, 2017a), eGovernment (UN, 2018), the use of information and communication technologies (WEF, 2018) as well as the commitment to cyber security (ITU, 2017b). The demonstration of the framework shows the complex nature of the forming of the indicators. The comprehensive context and the purpose of the use of the indicators shall guide the forming of indicators.

Strategic management is one of the purposes to use indicators. The paper applies the referred framework and the results of its demonstration in a case study about the governing of the digitalization resources and activities of the regional authorities. The case study was related to a major structural reform. The target of the reform was to form and launch the operations of new administrative structure, autonomous counties. The reform was supposed to cover the structure, services and funding of health and social services. In addition, the some of the tasks of the central government and the municipalities were planned to be transferred to the counties. The central government financed the planning and was supposed to finance the operating of the counties. The aims of the reform were to provide the citizens and inhabitants with more similar services, to reduce the variations in people´s health, and to curb the rising costs. The means to attain these aims included the more efficient use of information technology. The reform was cancelled in March 2019 (Regional Reform, 2019)

The empirical data of the case study included the ICT costs, digitalization efforts, shared ICT services and digital security situation of the regions. A group of regional authorities and public ICT agencies whose aim was to l provide the regions with shared ICT services gathered the empirical data in the beginning of 2019. The means of the reform included the co-creation of new types of digital processes and services in collaboration and with the citizens and the business actors as well as with the central government. This was considered to require collaboration between the regions and with the central government as well as with the citizens, the business actors and national and global ICT service providers and the security authorities.

Finally, the paper outlines the results of the analysis of the empirical data. The central government authorities analyzed the empirical data for the simulation of the financial negotiations between the central government and the regions. The results of the case study show that the framework supported the outlining of the contents of the empirical data so that both the digitalization and digital security aspects were concerned and visualized. In addition, the study seemed to raise the awareness of the digital security requirements. The authorities will apply the results of the analysis for the governing of the regions.

## 2. The balanced digitalization and digital security framework

Figure 1 illustrates the balanced digitalization and digital secure framework. It consists of a group of complex and emergent entities adapting to their environment over time (Holland 1996). A social system is, e.g., government, a regional authority, a business actor or a citizen or a group of all or some of them. A social system gives feedback as indicators. They are applied for adjusting the digitalization and digital security efforts. Parsons (1951) states that a social system has an initial and a goal state. In addition, he argued that the interaction orientation of the system is internal and external. In the spirit of the complex adaptive systems theory (Holland 1996) it can be argued that the initial state is being shaped to the goal state by information flows in the framework. Information is flowing continuously through the adjusting of digitalization and digital security efforts to the digital processes and services of a social system and as indicators to the adjusting function.

Figure 1 shows how the coherent balance is achieved by adjusting the digitalization and the digital security efforts in parallel (Kuusisto & Kuusisto 2017). As a result, digitalization and digital security are converging. This convergence guides the designing and implementing of the digital processes and services in such a way that both the digitalization target level and the security requirements can be reached.

As outlined in Figure 1, the indicators have to address digitalization and digital security. The selecting of the indicators shall be implemented in the context of the actor that is under concern, e.g., the government or a region. The indicators selected shall be relevant for the case and they shall be balanced with each other, as well. The government authorities at the national level can apply international digitalisation indexes and the cyber security situation indexes for the selecting of the indicators (Kuusisto & Kuusisto 2017). The international indexes that can be applied at the national level include UN (2018) eGovernment survey, ITU's ICT Development Index

(IDI) (2017a), World Economic Forum's (2018) Network Readiness Index, ITU's (2017b) Global Cybersecurity Index and Estonia's National Cyber Security Index (NCSI, 2019). Both the digitalization and cyber-security indicators have to be applied for balancing the digitalization and digital security efforts.

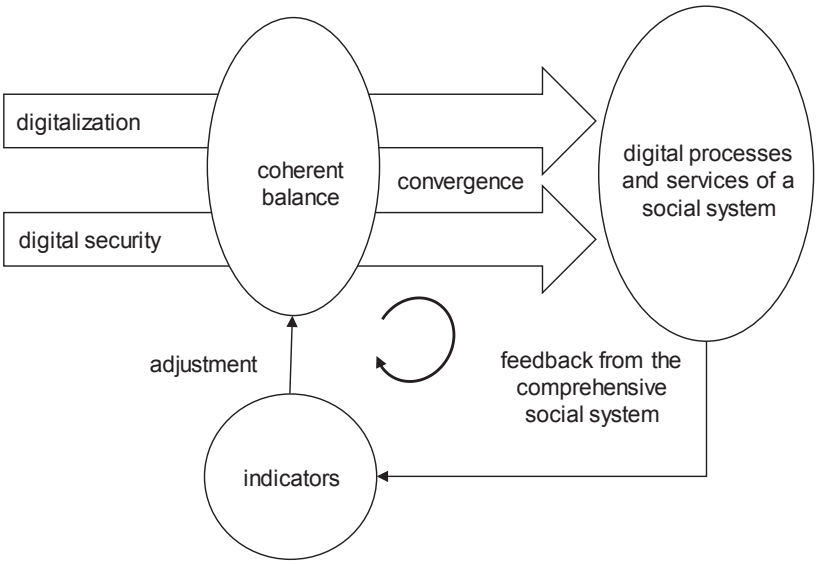


**Figure 1:** The balanced digitalization and digital security framework

UN (2018) eGovernment survey consists of eGovernment development index and eParticipation index. ITU's (2017b) Global Cybersecurity Index contains legal, technical, organizational, capacity building, and cooperation views on the national cyber-security. The aim of Estonia's NCSI (2019) is 'to measure the preparedness of countries to prevent cyber threats and manage cyber incidents'. The categories of the index are: Cyber security policy development, cyber threat analysis and information, education and professional development, contribution to global cyber security, protection of digital services, protection of essential services, E-identification and trust services, protection of personal data, cyber incidents response, cyber crisis management, fight against cybercrime and military cyber operations. The results of the surveys by these indexes can be applied for identifying the major phenomena and improvement needs of a country.

## 3. The demonstration of the balanced digitalization and digital security framework

The paper demonstrates the framework by applying UN (2018), ITU (2017b) and NCSI (2019) indexes. NCSI's Digital Development Level (DDL) is based on ITU (2017a) and WEF (2018). In this paper, UN (2018) and NCSI's (2019) DDL are referred as "digitalization" indicator sets and ITU (2017b) and NCSI are referred as "digital security" indicator sets. The selected indicator sets have been formed for the measuring of a certain aspects to the digitalization and digital security. The indicator sets are partly overlapping but all of them contain unique indicators and indicator weights. In addition, they use partly overlapping data sources. Obviously, the results and country rankings by these indicator sets are not similar.

Next, the paper focuses on the analysis of the results of these indicator sets. For the analysis, the scale of the country ranking results were converted. The first country in the ranking received score 100 and the last one received score 1. This aim of this was to visualize the country rankings in a comparable way. Ten countries were included in the visualization of the analysis. Figures 2 and 3 show the results of the digitalization indicator sets. The countries are presented in Figures 2, 3, 4, and 5 in the order of the country ranking results of the UN eGovernment Survey (2018). Figures 4 and 5 show the results of the digital security indicator sets.

When comparing the abstract patters that Figures 2 and 3 outline, it can be observed that these patterns are alike. However, the country ranking results of UN eGoverment Survey (2018) visualized in Figure 2 and NCSI's (2019) DDL visualized in Figure 3 are clearly not similar. The contents of these indicator sets have to be known for understanding what the indicators measure and what causes the differences in the country ranking results. The results should not be used for strategic-level decision making without understanding the contents of the indicators and source data.

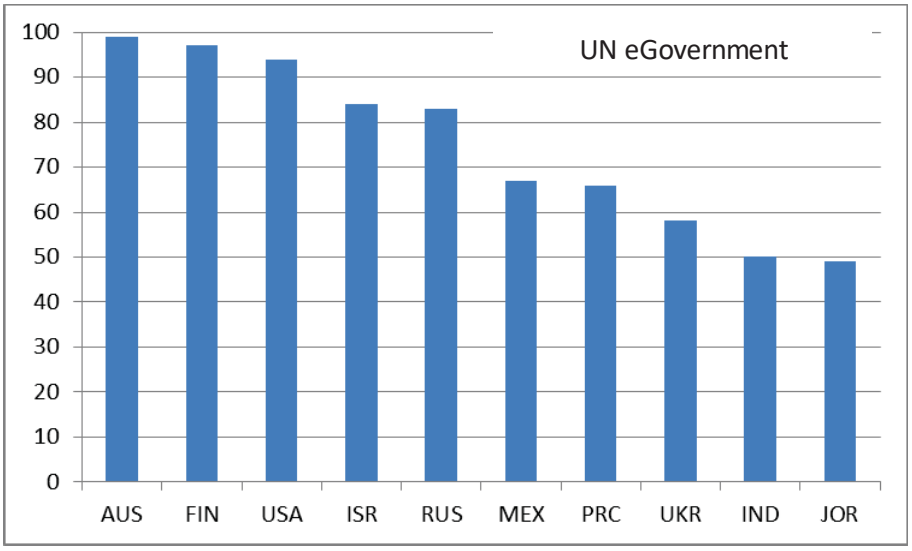


**Figure 2:** UN eGovernment Survey (2018), digital services indicator set

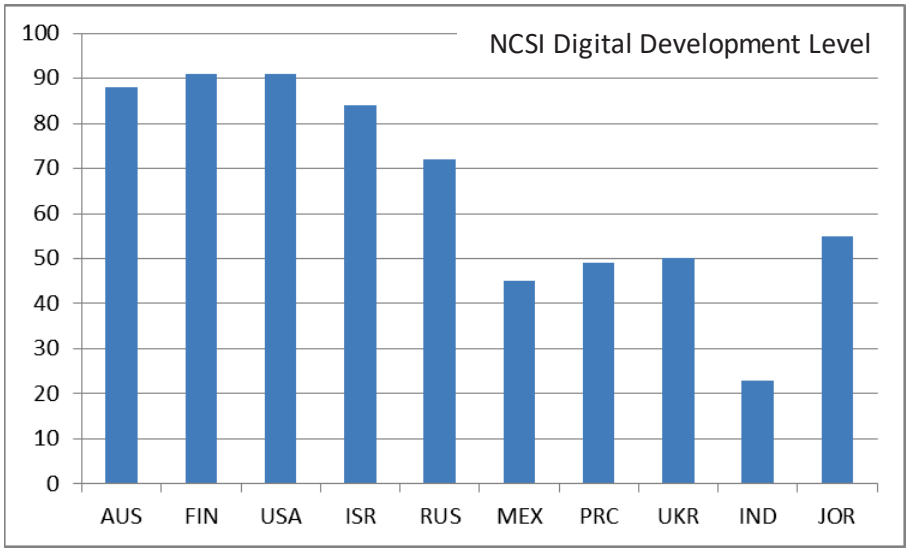


**Figure 3:** NCSI's (2019) Digital Development Level, digital services indicator set

The country ranking results of ITU Global Cybersecurity Index (2017b) visualized in Figure 4 and National Cyber Security Index (2019) results visualized in Figure 5 are somewhat different. The country positions vary more in these rankings than in the digitalization rankings. This may just be a coincidence. The sample data sets are quite small. On the other hand, the contents of the indicator sets and the way the evaluations are implemented are different. Therefore, the differences in the ranking results might indicate that the complex security evaluation concepts are not yet internationally defined, organized and regulated to a sufficient level.

As a conclusion, it can be observed that the country positions in the rankings vary more than just faintly. In addition, the correlation between the country rankings of the digitalization and digital security indicator sets is not complete. A hypothesis can be made that some countries have a noticeable unbalance between digitalization and digital security. In addition, it can be assumed that countries are directing cyber security efforts based on their national focus.

The very modest analysis above aims demonstrating that when planning and using indicators for supporting governance and management, a thorough analysis is needed for selecting or forming relevant and suitable indicator sets. At very general level, an indicator set should serve the context under concern and have proven balance between digitalization and digital security aspects.

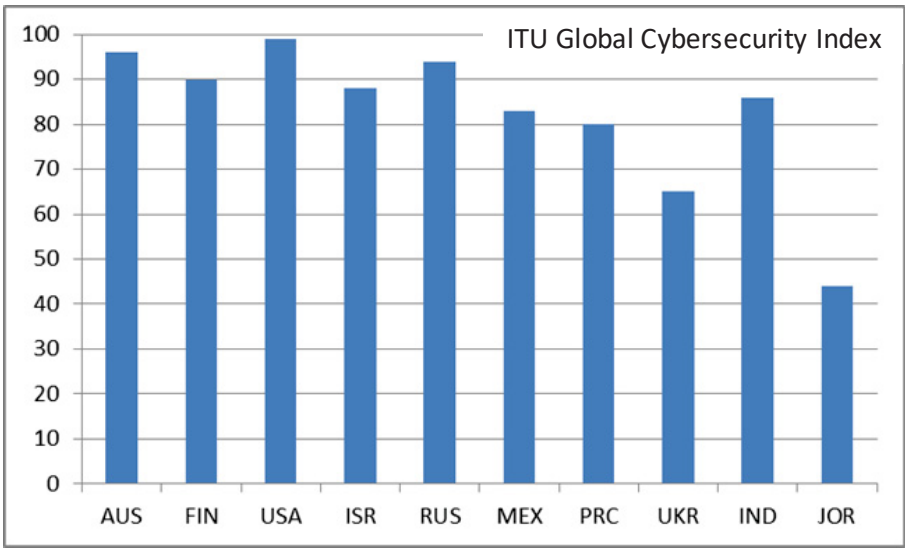


**Figure 4:** ITU Global Cybersecurity Index (2017b)

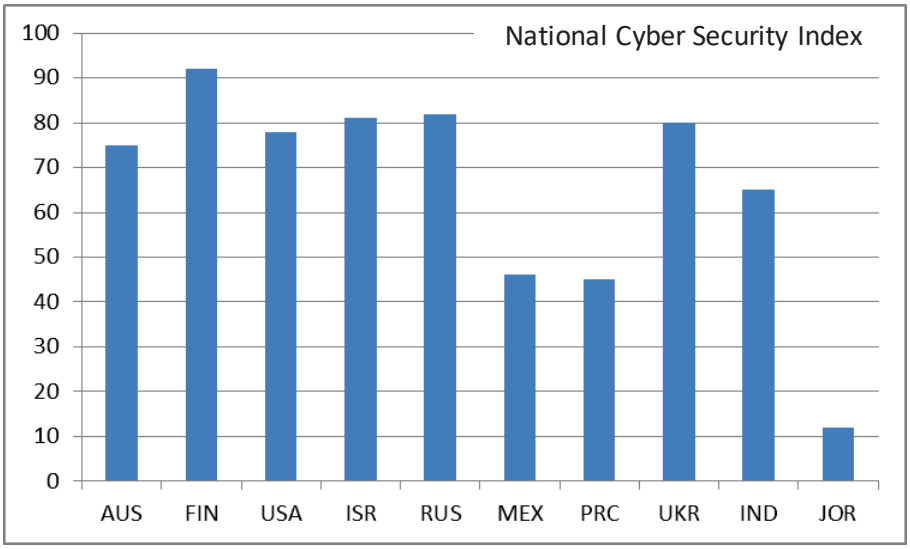


**Figure 5:** National Cyber Security Index (2019) results

As noted before, the balance between digitalization and digital security is relevant. The security level should be as high as the value of security to the organization require and the digitalization efforts are targeting. Over-digitalization leads to security gaps and over-security cause unnecessary costs. The more relevant both of the aspects are the more influential the organization is. When forming the indicators, we should be aware of the required service and security levels, the nature of the actor's activity and the overall context where the interacting actors are performing their activities in the digital world. When using the indicators, we should explicitly know how they are formed and what data they are using. The indicators shall be constructed to be relevant in the actor's governance, development and management context. Next, we demonstrate briefly how these simple principles succeeded in the case of aiming to develop the first attempt to form digital services - digital security overall service level and their internal balance in context of a major government reform.

## 4. Regional authorities case study

The balanced digitalization and digital security framework and the results of its demonstration were applied in a case study. The aim of the case study was to illustrate the first efforts to outline the rough contents of indicators relevant for supporting the governance, development, planning and management of the regions digitalization and digital security activities. The case study consisted of the analysis of the ICT and digitalization situation data of the regions. The central government authorities defined the contents of the analysis and the data describing the situation of the regions. Some of the regional authorities preparing the major reform contributed to the content definitions as well. Seven public institutions or agencies were planned to design,

implement and produce the shared ICT services for the regions. These organizations contributed to the outlining of the content definitions too.

The authorities designed the contents of the situation data and data analysis by following the agile approach. First, the authorities studied some of the international and national eGovernment evaluations, ICT surveys and standards, and practices of a global consulting company. They decided to include the financial figures, the major digitalization efforts and information systems, and the digital security situation reports to the situation data. The categories of the situation data of the regions as well as the service providers were:

- The total estimated ICT budget in 2019,
- the major digitalization activities,
- the major development programs and projects containing digitalization efforts or ICT, and their costs,
- the major current information systems and their operating costs, and
- the survey of cyber and information security situation.

The total estimated ICT budget contained several categorizations formed according to the current global practices. These included categorization to the hardware, software, human resources and internal and external sourcing costs as well as to the maintenance and development costs. In addition, the previous year ICT costs were asked to be reported as Capital Expenditure (CAPEX) and operating expenses (OPEX). The regional authorities involved in the major reform created and collected the data in the beginning of 2019. The authorities collected the data based on the tasks and responsibilities of the regions. The shared ICT service providers delivered data about their current or future shared ICT services to the regions.

The major observation about the financial figures was that the quality of the data was low. The definitions of ICT costs were region specific. In addition, some of the regions were not able to collect the required financial figures at all. Therefore, the central government authorities could not assess or compare the digitalization situations of the regions based on these figures. For example, there were several reasons for a high value in the total ICT costs per inhabitant of a region compared to the average ICT costs per inhabitant. These reasons included a high digitalization degree as well as duplicate information systems. Thus, the central government authorities considered that the financial data are insufficient, inaccurate and incomplete for the statistical analysis.

The central government authorities considered that the study of the digitalization efforts of the regions improved their awareness of the digitalization degree of the regions. The regions implementing or already proving the personnel and the inhabitants with the modern health care systems are obviously proceeding in digitalization. The analysis of the catalogues of the major current information systems, however, did not have a significant impact on the awareness of the digitalization degree.

The major observation of the cyber and information security survey of the regions was that the management, guidelines and practices of the health care organizations meet the basic level requirements. The assumption is that the survey improved the cyber and information security awareness of the regional authorities that were preparing the major reform. In the future, the central government authorities could govern the regions to extend the cyber and information security culture of the health care authorities to the other regional functions.

The major observations of the shared ICT service providers' situation data show that the maturity of the service provider and the phase of the life cycle of a digital product or service explains well the accuracy of the financial figures. This applies to the level of the cyber and information security as well. Novel organizations launched a few months ago had not yet formed the region-based commissioning plans of their services and so they could not estimate region-based costs of the shared services or products. In addition, they had not established the risk assessment based cyber and information security controls. A minor observation was that many of the shared ICT service providers reported that they had not exercised their contingency plans. This was not widely recognized before the survey. The assumed benefit of the collecting and analyzing of the situation data is that it increases the cyber and information security awareness of the regional authorities.

In addition to the data gathered from the regions and shared ICT service providers, the central government authorities decided to pilot the use of The Digital Economy and Society Index (DESI, 2019) in the regional level. DESI has five dimensions: Connectivity, Human Capital, Use of Internet Services, Integration of Digital

Technology and Digital Public Services. Statistics Finland defined a regional level pilot DESI with three dimensions that are relevant at the regional level: Connectivity, Human Capital and Use of Internet Services. The method and results are described in (MOF, 2019). The regional DESI pilot has the inhabitant view on the digitalization degree of a region. It illustrates the digital potential of the regions. The results of the regional DESI pilot are shown in Figure 6. As visualized in Figure 6, some of the regions have challenges in their digital economy. The more detailed study of the values of the composite regional DESI indicator dimensions (MOF, 2019) shows that especially the connectivity dimension has low values on some of the regions.

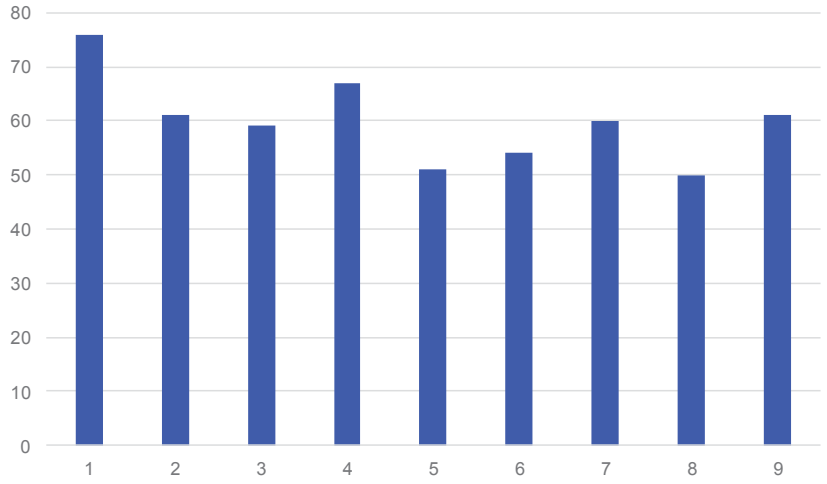


**Figure 6:** The digital potential of regions (MOF, 2019)

The regional authorities and the shared ICT service providers were involved the planning of a major structural reform. They were acting in a complex, evolving environment that yields diversity. The financial impacts of digitalization and digital security efforts are divergent. This challenged the collecting and analysis of the situation data. The aim was, however, that the publishing of the financial figures, digitalization efforts and digital security situation of the regions would adjust the coherent balance of the digitalization and digital security activities of the regions. The divergent definitions and approaches of the basic concepts, terms, and services would convert to understanding that is more similar. As a result, the regions would have secure shared digital services.

However, the case study showed that it is crucial to be able to select or form the indicators in such a way that they describe the actors' potential to develop and implement digital services and assure their security. This requires knowledge and competence about the indicators and their interpretation.

## 5. Conclusions

This paper refers to a theoretically motivated approach: the balanced digitalization and digital security framework outlined in Figure 1. It shows how the coherent balance of digitalization and digital security is gained by the joint adjusting of the digitalization and digital security efforts. This requires the development of the digital services and digital security in parallel. In addition, the governing of the development needs to be supported by accurate enough and relevant governance toolsets understood and accepted by all the actors involved. The result as its best is the convergence of digitalization and digital security for the governing of the design, implementation and providing of the digital services of society.

The digital services shall be considered as a social system - the system of relevant action by relevant actors in the defined context supported by technological structures and services. Theoretically, this can be considered as a complex adaptive system (CAS) and treated as one in ever evolving context. Thus, the balanced digitalization and digital security framework consists of a group of complex and emergent entities adapting to their environment over time. It will help to identify the most relevant development issues during that evolution. This social system gives feedback as indicators. They shall be used for directing the adjustment of the digitalization and digital security efforts. The nature and the origin of the data of the indicators are critical. It is obvious that the content and the selection of the indicator data will change during the system evolution. The indicator system shall be considered as a part of the strategic guidance of the comprehensive governance.

## References

DESI (2019) *The Digital Economy and Society Index*, Retrieved on the 22nd of February 2019 from https://ec.europa.eu/digital-single-market/en/desi

Gartner (2019) *IT Glossary*. Retrieved on 3rd of January 2019 from https://www.gartner.com/it-glossary

Habermas, J. (1984) *The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society*, Boston, MA: Beacon Press.

Habermas, J. (1989) *The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason*, Boston, MA: Beacon Press.

Holland, J.H. (1996) *Hidden Order: How Adaptation Builds Complexity*, Cambridge, MA. Perseus Books.

International Telecommunication Union (ITU) (2017a) *ICT Development Index.* Retrieved on the 30th of April 2019 from http://www.itu.int/net4/itu-d/idi/2017/index.html

International Telecommunication Union (ITU) (2017b) *The Global Cybersecurity Index*. Retrieved on the 3rd of January 2019 from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Kuusisto, R. (2004) *Aspects on availability*, Edita Prima Oy, Helsinki, Finland.

Kuusisto, R. (2008). *Analyzing the Command and Control Maturity Levels of Collaborating Organizations*. In: Proceedings of 13th International Command and Control Research and Technology Symposium (13th ICCRTS), Bellevue, WA, USA, 17-19 June 2008

Kuusisto, T., Kuusisto, R., Roehrig, W. (2015) "*Situation Understanding for Operational art in Cyber Operations*". In Abouzakhar, N. (ed.) Proc of the 14th European Conference on Cyber Warfare and Security ECCWS-2015, Hatfield, UK, 2.-3.7.2015, pp. 169-178, Published by Academic Conferences and Publishing International Limited Reading, UK 44-118-972-4148, www.academic-publishing.org

Kuusisto, T., Kuusisto, R. (2017) "*Security Culture in Digital Inter-Organizational Ecosystems*". In Scanlon, M. & Le-Khac, N.-A. (eds.) Proc. of the 16th European Conference on Cyber Warfare and Security, ACPI, 29-30 June 2017, pp. 216-223

Merriam-Webster (2019). Merriam-Webster online dictionary. Retrieved on the 3rd of January 2019 from https://www.merriam-webster.com

Ministry of Finance (MOF) (2019), *DESI results at regional level*, Retrieved on 19th of February 2019 from https://alueuudistus.fi/artikkeli/-/asset_publisher/maakuntien-ict-tilannekuvaa-taydennetty-digitalisoitumisindikaattorilla, in Finnish

NCSI (2019). *National Cyber Security Index*. Retrieved on the 3rd of January 2019 from https://ncsi.ega.ee/methodology/

Parsons, T. (1951) *The Social System*, Free Press, Glencoe, IL.

Regional Reform (2019). *Regional Government, Health and Social Services Reform*. Retrieved on the 30th of April 2019 from www.regionalreform.fi

United Nations (UN) (2018*) E-Government Survey 2018, Gearing E-Government to Support Transformation Towards Sustainable and Resilient Societies*. United Nations, Economic & Social Affairs. Retrieved on the 3rd of January 2019 from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

World Economic Forum (WEF) (2018) *Network Readiness Index.* Retrieved on the 30th of April 2019 from http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/

an Honours Degree in Management from Henley University and a Master's and PhD in Informatics from the University of Johannesburg - specialising in strategies for cyber counterintelligence maturity and the security of cyberspace. He has published various academic papers on cyber strategies and cyber counterintelligence maturity. His professional certifications include CISSP, CISM and CCISO.

**Dr. Connie Justice** has over 30 years' experience in cybersecurity, computer, and systems engineering. She designed courses in cybersecurity curriculum to NSA/DHS Center of Academic Excellence and NIST National Initiative for Cybersecurity Education standards. Research areas include: fake news, industrial controls risk, experiential learning, information and security risk management, digital forensics.

**Fredrick Kanobe** was PhD candidate at Tshwane University of Technology, South Africa. His research domain is ICT4D.

**Mrs. Eleni Kapsokoli** is PhD Candidate in University of Piraeus, Department of International and European Studies, Greece. She also holds a bachelor degree from the National and Kapodistrian University of Athens at the faculty of Political Science and Public Administration. She earned her Master's Degree on International Relations and Strategic Studies at the Panteion University of Social and Political Sciences. Her main research interests include international security, terrorism, cybersecurity and cyberterrorism. She is also a researcher in the Institute of International Relations (I.I.R). She is also a PhD Fellow at the European Security and Defence College (ESDC).

**Martti J Kari** is university teacher and PhD student of cyber security in Jyväskylä University, Finland. He retired as colonel from Finnish Defense Intelligence in the end of year 2017. His last post was Assistant Chief of Defense Intelligence. He has MA in Russian language (1993) and literature and MA in cyber security (2017) in Jyväskylä University. Kari has worked as a university teacher from the beginning of year 2018 In Jyväskylä University. He is specialized in Russian cyber and hybrid warfare.

**Kaur Kullman** is researching at the US ARL whether stereoscopically perceivable 3D data visualizations would be helpful for cybersecurity analysts, incident responders and other operational roles. He's been in IT since '90s, focusing on cybersecurity since late '00s. His interests are hands-on technical (OS-hardening, malware analysis, pentests), while his duties at EISA were more various.

**Kautsarina** is a government researcher at Ministry of Communication and Information Technology (MCIT), Republics of Indonesia since 2009. She also works as an ISO 27001 Lead Auditor for public institution since 2011. She is involved in developing policy research and ICT master plan. Now she is full-time PhD student at Computer Science Faculty, University of Indonesia. Her interest is about information security awareness improvement for end-user.

**Anthony Keane**, MSc, PhD has a background in astrophysics research and computer science and is currently the Head of the School of Informatics & Engineering in the Technological University Dublin, Ireland. He is also a Principal Investigator in the Cyber Security Education & Research Centre with interests in Cyber Bullying, Cyber Warfare and Cloud Forensics.

**Thorsten Kodalle** is lecture on security policy at the Command and Staff College of the German Armed Forces with a special focus on NATO, Critical Infrastructure and Cyber. He has a diploma in Social Science, assignments as a youth information officer, in the MoD, lecture on management and leadership and supported for several years computer assisted exercises at the Command and Staff College with constructive simulation. He is a member of the NATO research task group "Gamification of Cyber Defense/Resilience", an experienced facilitator of manual wargaming on the operational level for courses of action analysis, for operational analysis, operations research, serious gaming and especially for matrix wargaming.

**Tuija Kuusisto** is a Senior Ministerial Advisor at Ministry of Finance and an Adjunct Professor at National Defence University and University of Jyväskylä in Finland. Her expertise covers information analysis and management for decision-making, as well as information and cyber security strategies and policies. She have contributed to several international research and experiment projects and working groups organized by EU, UN and OECD. She has about 70 scientific publications in international and national journals, conference proceedings and books.