LAUREA AMMATTIKORKEAKOULU University of Applied Sciences www.laurea.fi

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Rajamäki, J. & Knuuttila, J. (2015) Cyber Security and Trust: Tools for Multi-agency Cooperation between Public Authorities. In Ana Fred, Jan Dietz, David Aveiro, Kecheng Liu, Joaquim Filipe (Eds.) Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2015)– Volume 3: KMIS. Lisbon: SCITEPRESS Science and Technology Publications, 397-404.

doi: 10.5220/0005628803970404

CC BY-NC-ND 4.0

LAUREA

Cyber Security and Trust
Tools for Multi-agency Cooperation between Public Authorities

Jyri Rajamäki[1] and Juha Knuuttila[2]
[1]*Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland*
[2]*Turku University of Applied Sciences, Lemminkäisenkatu 30, FI-20520 Turku, Finland*

Keywords: Cyber Security, Disaster Relief, Multi-agency Cooperation, Multiple Case Study, Public Protection, Resilience, Resiliency, Software-intensive Systems, Trust, Trust-building.

Abstract: Functions vital to society, such as public protection and disaster relief (PPDR), are increasingly dependent on networks, electricity and data processing infrastructure. Incidents such as natural hazards and organized crime do not respect national boundaries. As a consequence, there is a need for European collaboration and information sharing related to public safety communications, and information exchange environments, technologies and procedures. This multiple case study analysis collects together research results from four earlier research projects. The main research question is: How can cyber security and trust-building be understood and designed as being tools for multi-agency cooperation between PPDR agencies? The results show that 'trust' could be seen as the main issue with regard to multi-agency cooperation. Cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. It is important to complement the currently dominating 'cyber security as a barrier' perspective by emphasizing the role of 'cyber security as an enabler' of new interactions and services - and recognizing that trust is a positive driver for growth. Safety and security issues are increasingly dependent on unpredictable cyber risks. Everywhere present computing means that PPDR agencies do not know when they are using dependable devices or services and there are chain reactions of unpredictable risks. If cyber security risks are not made ready, PPDR agencies will face severe disasters over time. Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world.

1 INTRODUCTION

In major disasters, not a single organization can work alone. Hence, co-operation is extremely critical between actors. The working parties should not simply trust and rely on their own resources. Regardless, only a few organizations possess all the required areas of expertise in a large-scale incident or disaster. Information sharing at the organizational level is required in order to achieve a working relationship between the actors. This requires actual and operational interoperability between public protection and disaster relief (PPDR)—in reality in the field, not only in the form of an official agreement but on a much larger scale (Akella et al., 2010).

The term 'public protection and disaster relief' is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical services and disaster recovery services for the citizens of the political sub-division of each country. These individuals help to ensure the protection and preservation of life and property. PPDR agencies are responsible for the prevention of and protection from events that could endanger the safety of the general public (Baldini, 2010). Such events could be natural or man-made. The main PPDR functions include law enforcement, emergency medical services, border security, protection of the environment, firefighting, search and rescue, and crisis management. One major challenge in defining a classification of PPDR agencies at the European level is that, due to the non-homogenous historical development of PPDR, similar organizations have different roles in different countries (Baldini, 2010).

Public protection keeps the wheels of secure daily life turning. When the basic functions of society are in order it is possible to return to normal life after

Rajamäki, J. and Knuuttila, J..
Cyber Security and Trust - Tools for Multi-agency Cooperation between Public Authorities.
In *Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2015) - Volume 3: KMIS*, pages 397-404
ISBN: 978-989-758-158-8
Copyright © 2015 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

crises without losing the firm ground on which society rests. Disaster relief becomes evident when something goes badly wrong; for example, a major accident occurs. However, the functions vital to society must be secured in all times: in normal conditions as well as in crises.

PPDR agencies face interoperability issues at all levels (technical, operational, legal and social) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe but also collective responses to threats and crisis must be enabled in an increasingly interconnected network. In addition, the organizations stand to gain from the interoperability functionality in their routine work. On one hand, Europe is a patchwork of languages, laws and diverse cultures and habits that can change abruptly across borders. On the other hand, even in the same country, each PPDR agencies develops its own technologies and operational procedures. For efficient operations, many serious challenges need to be addressed, including public safety communication (PSC) systems (which are not compatible even when they use the same technology) and differing procedures as well as inadequate language skills in cross-border cooperation.

PPDR operations are increasingly more dependent on information and communication technology (ICT) systems and services. Incidents such as natural hazards do not respect national boundaries, but most PPDR operations are based on national organizations. As a consequence, there is an increased need for European collaboration and information sharing related to PSC and information exchange technologies and procedures. EU has funded dozens of research projects aiming towards better technological interoperability, but their results have been minor, because distrust – not technology – is the biggest problem to interconnect different organizations' ICT systems together (Kämppi et al., 2014).

The objective of this multiple case study analysis (cf. Yin, 2009) is to develop an improved understanding of information sharing environments to foster cross-sectorial and cross-border collaboration between PPDR agencies. With regard to multi-agency cooperation between PPDR agencies, the paper collects together research results from four earlier research projects in which the first author acted as the national coordinator and responsible scientific supervisor. The main research question is: How can cyber security and trust building be understood and designed as being tools for multi-agency cooperation between PPDR agencies?

This paper has four sections sections, including the foregoing introduction.. A theoretical framework is presented in the second section where there are an introduction to trust issues, information infrastructures, resilience and software-intensive systems. The third section presents the four empirical cases, from which the results and findings of this paper are based on, and the last section makes cross-case conclusions.

2 THEORETICAL FRAMEWORK

2.1 Trust Issues in PPDR Operations

Trust is the base that every joint- and co-operation action is built on. Simplistic way to estimate trust is "trust/distrust", which rarely describes the actual situation accurately. For PPDR to function, some level of trust towards the general public, audience, the (paying) customer as well as performers and other staff is needed. For any meaningful interaction, basic level trust towards the other must exist. A private security guard expects to be taken seriously by the authorities when contacting and vice versa. The basic level of trust is interwoven in the roles we have and take while interacting. Mostly these are social norms but in some cases these expectations may be written down as guidelines or law - contracts of sort. Whether written down or not, these are the generally excepted norms that by which we set our trust (Tourish and Hargie, 2004).

The general acceptance of these social contracts makes them formal. This 'formalized trust' is the level we usually operate between people and organizations we do not really know (Hofstede, 1991). Formalized trust is often forced and rarely flexible. Trust between organizations is mostly formalized and the formal level is easily seen as the maximum. An example of this is to limit the access and communication to formal channels and methods. Informal trust stems from actually knowing the other and is usually stronger but more prone to fluctuation. The gap between needed levels of trust, for example for cooperative use of resources, can be overcome (at least locally) by personal informal trust. Informal trust was accepted as sufficient level to form the joint security management in the areas that seemingly were to most efficiently and smoothly run, cf. Jarvenpaa and Majchrzak (2008).

2.2 Theory of Borders

It is becoming apparent that effective border security

can only result from effective cross-national collaboration (Henningsson et al., 2011). Accordingly, trust, information sharing, technical infrastructure and cultural understanding become the cornerstones of successful cross-border collaborative efforts (Luis et al., 2013).

Navarrete et al., (2009) bring together Brunet-Jailly's (2009) theory of borders and definitions of cross-boundary information sharing to develop a framework that incorporates the information sharing and technology dimension with the economic, political and cultural contextual factors impacting border regions. Their framework integrates the four dimensions adapted from Brunet-Jailly (summarized in Table 1) with current research in cross-boundary information sharing (summarized in Table 2).

Table 1: Theory of borders dimensions.

Dimensions	Description
Market forces and trade flows	Flows of good, people and investments across borders
Policy activities of multiple levels of governments on adjacent borders	Link that must be established between, in one hand, local, provincial, state, and central governments, and in the other hand, task specific public and private sector organizations
The particular political clout of cross-border communities	Local civic and political organizations and individuals on the border
Culture of cross-border communities	Sense of community, common language, religious and socio-economic background of a specific border region

Table 2: Technical and social aspects of information sharing.

Component	Description
Trusted Social Networks	Networks of social actors who know each other and trust each other.
Shared Information	Sharing of tacit and explicit knowledge in the form of formal documents, informal talks, e-mail messages, faxes, etc.
Integrated Data	Integration of data at the level of data element standards and/or industry/community data standards (e.g. XML).
Interoperable Technical Infrastructure	Systems that can communicate with each other at the hardware/operating system level.

2.3 Design Principles for Information Infrastructures

There has been a gigantic shift from a hardware product based economy to one based on software and services. This has also been the fact with regard to PPDR. From every indication, the growth of the software layer, in size and percentage of the overall systems, will be the future trend. The information infrastructure (II) literature has addressed the challenges of realizing large-scale technological systems (Edwards et al., 2009; Hanseth and Lyytinen, 2010; Monteiro and Hanseth, 1996). Large-scale information systems are not stand-alone entities but rather are integrated with other information systems and communication technologies as well as with other technical and non-technical elements. This approach is relevant for analyzing the domain of critical information infrastructures.

Hanseth and Lyytinen (2010) have synthesized their study's insights into a normative design theory for IIs, distinguishing between two generic challenges: 1) The ''bootstrap problem'' addresses the establishment of a novel II. Since an II gains much of its value from its large and diverse user base and components, the fact that initially the user community is non-existent or small precludes the fact that the infrastructure can offer these benefits. 2) The ''adaptability problem'' relates to the further growth and expansion of an II where unforeseen demands, opportunities, and barriers may arise.

Aanestad and Jensen (2011) have studied IIs in healthcare. According to them, large-scale and long-term stakeholder mobilization is a core challenge when realizing nationwide information infrastructures for public organizations. They continue that the implementation strategy of such IIs must deal with the multiple stakeholders and be able to mobilize and coordinate them. A modular implementation strategy, made possible by appropriate modularity of the solution, allows the implementation to be organized in a way that does not require wide-spread and long-term commitment from stakeholders initially. They argue that "solutions that provide immediate use value by offering generic solutions to perceived practical problems, balance the stakeholders' costs and benefits, and solve a problem with minimal external dependencies, can avoid some of the dilemmas often associated with large-scale IIs." Their research illustrates the dangers of introducing requirements that are too high for stakeholder mobilization, and the notions of stable intermediary forms and modular transition strategies may help decision-makers to pursue other avenues when planning large-scale implementation projects (Aanestad and Jensen, 2011).

In the future world of pervasive computing and ubiquitous cyber-physical devices, it will be essential that IT artifacts and the integrated systems containing these artifacts be reliable, adaptable, and sustainable (Hevner and Chatterjee, 2010). Design for software-

intensive systems (SIS) should draw its foundations from multiple research disciplines and paradigms in order to effectively address a wide range of system challenges. The most important intellectual drivers of future science of design in SIS research will be dealing with complexity, composition and control (Hevner and Chatterjee, 2010). Hanseth and Lyytinen (2010) adopt the viewpoint of designers: "how to 'cultivate' an installed base and promote its dynamic growth by proposing design rules for II bootstrapping and adaptive growth." Within their design rules, the II designers would have to prefer continuous, local innovation to increase chaos and to apply simple designs and crude abstractions. This change is not likely, as design communities are often locked into institutional patterns that reinforce design styles assuming vertical control and complete specifications (Hanseth and Lyytinen, 2010).

2.4 Resilience for Cyber Systems

The National Academy of Sciences (2012) identifies four event management cycles that a system needs to maintain to be resilient: 1) Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack). 2) Absorb: Maintain most critical asset function and service availability while repelling or isolating the disruption. 3) Recover: Restore all asset function and service availability to their pre-event functionality. 4) Adapt: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient.

The Network-Centric Warfare (NCW) doctrine (Alberts, 2002) identifies four domains that create shared situational awareness and inform decentralized decision-making: 1) Physical: Physical resources and the capabilities and the design of those resources. 2) Information: Information and information development about the physical domain. 3) Cognitive: Use of the information and physical domains to make decisions. 4) Social: Organization structure and communication for making cognitive decisions.

Linkov et al., (2013) combined the event management cycles and NCW domains to create resilience metrics for cyber systems. Their approach integrates multiple domains of resilience and system response to threats through integrated resilience metrics; however, study of systems as multidomain networks is relatively uncommon. Links across domains are likely to affect the network's resiliency and should be assessed using network science tools (Abdelzaher and Kott, 2013).

2.5 Resilient Software-intensive Systems

Modern societies are highly dependent on different critical software-intensive information systems that support society. Designing security for these information systems has been particularly challenging since the technologies that make up these systems. Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how these resilient software-intensive systems are conceptualized, built and evaluated (Hevner and Chatterjee, 2010). Rajamäki and Pirinen (2015) are developing a design theory (DT) for resilient SISs (DT4RSIS) so that communities developing and operating different information technologies can share knowledge and best practices using a common frame of reference, as summarized in Figure 1.

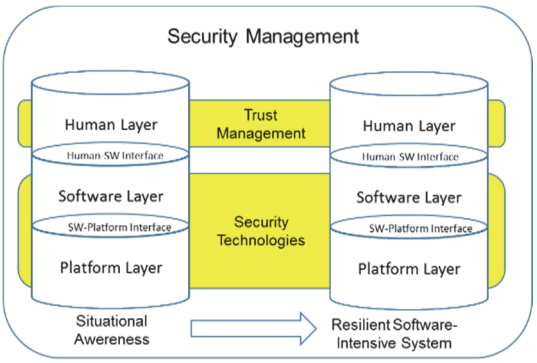

Figure 1: Constructs of design theory for resilient software-intensive systems (Rajamäki and Pirinen, 2015).

According to DT4RSIS (Pirinen and Rajamäki, 2015), resiliency means that a system or infrastructure is able to adapt to changing conditions, in the case of information security, based on run-time situational awareness and a priori risk analysis. Situational awareness involves being aware of what is happening around one to understand how information, events, and one's own actions affect the goals and objectives, both now and in the near future. The most important enablers of situational awareness are observations, analysis, visualization, and cyber-policy of the government. Security technologies include all technical means towards cyber security, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment. Security management and governance covers the human and

organizational aspects of information security. Its focus areas include: 1) Security policy development and implementation, and 2) Information security investment, incentives, and trade-offs. Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization's information assets that do preserve (Pirinen and Rajamäki, 2015).

3 RESEARCH CONTRIBUTIONS

This section briefly describes the results and lessons learned, with regard to cyber security and trust-building, from the four empirical cases that belong to this multiple case study analysis.

3.1 RIESCA

Rescuing of Intelligence and Electronic Security Core Applications (RIESCA) project (started 10/1/2007, ended 3/31/2010) was our first externally funded research and development project. It developed information security management techniques that can be used to ensure the proper functioning of critical systems in all circumstances. Particular attention was paid to the situation of moving from normality to a crisis situation and recovering from the crisis to a normal state (Pirinen and Rajamäki, 2010). The other aim was to develop different security management and communication systems for critical events, including mass events (Reivo et al., 2010), high-level political meetings (Ilander et al., 2010) and crisis situations (Ojasalo et al., 2009), and to assess methods for evaluating their functionality.

RIESCA had societal impacts; it implicated national and international discussions in the field of critical infrastructure protection. RIESCA aligned with the key concepts regarding the 1st EU-US Expert Meeting on Critical Infrastructure Protection (CIP). Furthermore, RIESCA partially contributed on the improvement of the national authorities' communities' network (TUVE). RIESCA aided in creation of public-private-partnerships (PPP) between the participators and external partners. RIESCA increased networking with international actors, regarding the Infragard system, which was presented to Finnish actors. RIESCA raised discussions on privacy of citizens, as there was lot of discussions about privacy versus traceability of person. RIESCA raised awareness of the weaknesses of different networks with regard to dependability of networks. Furthermore, participators of RIESCA actively collaborated to different security related standards and frameworks, such as the national "Vahti" group work and ISO/IEC standards.

3.2 SATERISK

The SATERISK (SATEllite-based tracking RISKs) project (started 9/1/2008, ended 12/31/2011) studied risks associated with satellite-based tracking, specifically whether the use of tracking generates additional risks (Rajamäki et al., 2012). SATERISK answered the following questions: Does satellite-based navigation and tracking involve risks? Do we know what the risks are now and what they will be in the future? Often new technologies will present opportunities for increased safety and security—and this is certainly true with satellite-based navigation and tracking—but they can also create new risks. It is important for the technology developers and end-users to clearly understand these risks and take steps to mitigate them. The project aimed at a situation where laws on positioning and tracking allow the use of machine to machine tracking devices across state and union borders. SATERISK brought new know-how at the international level to the European security field (Rajamäki and Knuuttila, 2013). SATERISK created new methods and development paths for positioning and tracking systems (Rajamäki, 2014). The widely used US-based Global Positioning System (GPS) and Russian-based Globalnaja navigatsionnaja sputnikovaja sistema (GLOSNASS) satellite positioning systems will soon get an EU counterpart and rival from Galileo. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. SATERISK also offered technological solutions to issues that arose while the project was under way (Happonen et al., 2009). SATERISK created new methods and development paths for positioning and tracking systems that address the risks and limitations that have been discovered (Rajamäki et al., 2015). These methods related to information security, signal interference and legal restrictions on tracking. Amongst safety and security professionals—both in the public and private sectors—where the risks could be high if they were not properly addressed—a special emphasis has been placed on the use of satellite-based tracking.

3.3 MOBI

The number of technical devices, applications and

services in emergency response vehicles (ERVs) has increased during the past few decades. This progression has also increased the volume of different user interfaces and generated new problems, e.g. vehicle airbags have less room to fill. Technical problems, especially with power consumption and cabling, have also been reported. The Mobile Object Bus Interaction (MOBI) project (started 9/1/2010, ended 31/3/2014) made essential feasibility studies towards a common ICT hardware and software infrastructure for all ERVs. This information infrastructure includes devices for voice and data communications, computers, screens, printers, antennas, and cables, and in addition, interlinking with factory-equipped vehicles' ICT systems is researched. MOBI project's approach was to divide ERVs' ICT systems into four layers that have the standardized interfaces. These layers are 1) a vehicle infrastructure and power management layer, 2) a communications layer, 3) a service platform and common services layer, and 4) an actor-specific services layer. Some aspects run through all layers, such as security, power efficiency and product safety regulations (Rajamäki, 2013).

Applying of social media has exploded, and the authorities from the advanced countries have taken these matters into account when developing their digital services for PPDR (Akhgar et al., 2013). People being first at the scene of the accident (involved and/or eyewitness) should be able to communicate with PPDR authorities who are able to receive social media and multimedia messages into their operative systems. Kantarci and Mouftah (2014) present a framework where Internet of things can enhance public safety by crowd management via sensing services that are provided by smart phones equipped with various types of sensors. Their trustworthy sensing for crowd management concept can enhance the utility of the public safety authority up to 85%.Unfortunately, many PPDR organizations see the Internet and social media only as an extra resource in which they can collect and transpose "material" to analyze it in their own systems. In practice, too strict data security regulations may rule out the mobile utilizing of digital services in the field. However, most often the biggest cyber threat is "insider threat" like Snowden and Manning cases indicate. When taken into account the Finnish cultural-ethnic environment, it could be invested in towards this security originated from end-users, rather than the strict technical data security by which the last 0.02% of confidence can be achieved (Tikanmäki et al., 2014).

3.4 MACICO

The problem behind the Multi-Agency Cooperation in Cross-Border Operations (MACICO) project (started 12/1/2011, ended 12/31/2014) was that PPDR agencies in different countries, sometimes even different agencies in the same country, use their own separate professional mobile networks based on fragmented technological implementations. Roaming, interoperability, or common operational procedures do not exist. But in crisis situations and cross-border operations, the need of safe and secure communication is obvious. MACICO found solutions to improve interoperability of communication on all levels: users, operating procedures, services, service providers, and technology. The objective was better communication between security authorities and organizations and better public safety (Kämppi et al., 2014).

PPDR agencies present-day digital systems do not support cross-border cooperation. In addition to technical challenges, the distrust between agencies (especially in law enforcement such as police) causes trouble. Unfortunately, this distrust also exists at the national level, and even between units of one organization. However, common digital systems and operational procedures could increase the trust between parties. The European Network of Law Enforcement Technology Services (ENLETS) was established as a sub-group of the Law Enforcement Working Party of the EU Council in 2008. ENLETS' vision is to be the leading European platform that strengthens police cooperation and bridges the gap between the users and providers of law enforcement technology. The core group members of ENLETS (The Netherlands, The United Kingdom, Finland, Belgium, Poland and the EU's presidency country) should develop common procedures to apply new law enforcement technology. In the future, these procedures could be extended to other European countries as well as other field of PPDR (Rajamäki, 2015).

4 CROSS-CASE CONCLUSIONS

From citizens' point of view, PPDR is one complex software-intensive system that consists of several different sub-systems, such as 112-services, law enforcement, emergency medical services, and firefighting and rescue services, as shown in Figure 2. All these sub-systems are further divided to many sub-sub-systems.

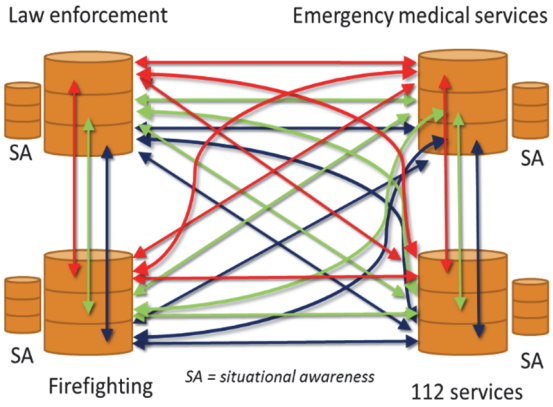

Figure 2: Complex software-intensive systems of PPDR sub-systems.

For returning privacy and trust in digital world, the targets could be summarized as follows: 1) Proactive – design for security. A proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries. 2) Self-healing – utilizing the toolbox. Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing. 3) Public awareness – increase trust. Enable seamless cyber security integration to every-day life. By efficiently utilizing tools and methods, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public awareness and understanding will move towards accepting cyber security as a natural element of a connected world.

Software-intensive systems consist of three layers: the platform layer, the software layer and the human layer. Every cyber-secure system consists of two SISs: the proper resilient system, and the situational awareness system that is the main prerequisite towards cyber security. A complex SIS is a system of software-intensive sub-systems, which platform layers compose a physical network, software layers compose a software network and human layers compose a social network, as shown in Figure 2. Trust should be systematically built up at all layers and networks. The resilient physical network (composed by blue arrows in Figure 2) is the basis on which the information sharing between different stakeholders could be created via software layers (green arrows). However, the trust inside social networks (red arrows) quantifies the pieces of information that will be shared, - and with whom.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resiliency focuses. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed. This requires information exchange between different stakeholders. The software-intensive situational awareness systems of different resilient systems compose similar networks than the proper resilient system (not figured in Figure 2). And always, when dealing with information exchange, the main question is "trust".

REFERENCES

Aanestad, M., Jensen, T. B., 2011. Building nation-wide information infrastructures in healthcare through modular implementation strategies. *The Journal of Strategic Information Systems*, 20(2), 161-176.

Abdelzaher, T., Kott, A., 2013. *Resiliency and robustness of complex systems and networks. Adaptive, dynamic and resilient systems.* Auerbach Publications, Florida

Akella, R., Tang, H., McMillin, B. M., 2010. Analysis of information flow security in cyber–physical systems. *International Journal of Critical Infrastructure Protection*, 3(3), 157-173.

Akhgar, B., Fortune, D., Hayes, R. E., Guerra, B., Manso, M., 2013. Social media in crisis events: Open networks and collaboration supporting disaster response and recovery, *IEEE International Conference on Technologies for Homeland Security*, pp. 760-765.

Alberts, D., 2002. *Information age transformation, getting to a 21st century military*. DOD Command and Control Research Program. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904.

Baldini, G., 2010. *Report of the workshop on "Interoperable communications for safety and security"*. Publications Office of the European Union,

Brunet-Jailly, E., 2005. Theorizing Borders: An Interdisciplinary Perspective. *Geopolitics*, 10, 633-649.

Edwards, P. N., Bowker, G. C., Jackson, S. J., Williams, R., 2009. Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems*, 10(5), 364-374.

Hanseth, O., Lyytinen, K., 2010. Design theory for dynamic complexity in information infrastructures: The case of building internet. *Journal of Information Technology*, 25(1), 1-19.

Happonen, M., Kokkonen, P., Viitanen, J., Ojala, J., Rajamäki, J., 2009. Jamming Detection in the Future Navigation and Tracking Systems. *16th Saint Petersburg International Conference on Integrated Navigation Systems*. Saint Petersburg, Russia.

Henningsson, S., Gal, U., Bjørn-Andersen, N., Yao-Hua, T., 2011. The Next Generation Information Infrastructure for International Trade, *Journal of theoretical and applied electronic commerce research*,

Vol. 6, No. 1.

Hevner, A., Chatterjee, S., 2010. *Design science research in information systems*, Springer.

Hofstede, G., 1991. *Cultures and Organizations*. London: McGraw-Hill.

Ilander, T., Toivonen, H., Meriheinä, U., Garlacz, J., 2010. Indoor Positioning for Nuclear Security. *Third European IRPA Congress.*

Jarvenpaa, S. L., Majchrzak, A., 2008. Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. *Organization Science*, vol. 19, 260-276.

Kantarci, B., Mouftah, H. T., 2014. Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things. *Internet of Things Journal*, IEEE, vol. 1, 360-368.

Kämppi, P., Rajamäki, J., Tiainen, S., Leppänen, R. (Eds.), 2014. *MACICO - multi-agent co-operation in cross-border operations*. Vantaa: Laurea.

Linkov,I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., Kott, A., 2013. Resilience metrics for cyber systems. *Environ Syst Decis*. DOI: 10.1007/s10669-013-9485-y.

Luis, FL, Derrick DC, Langhals B, Nunamaker JF., 2013. Collaborative cross-border security infrastructure and systems: Identifying policy, managerial and technological challenges. *International Journal of E-Politics (IJEP)*. 4(2), 21-38.

Monteiro, E., Hanseth, O., 1996. Social shaping of information infrastructure: On being specific about the technology. *Information Technology and Changes in Organizational Work*, 325-343.

National Academy of Sciences, 2012. *Disaster resilience: a national imperative*. Washington DC, United States. http://www.nap.edu/catalog.php?record_id=13457.

Navarrete, A.C., Mellouli, S., Pardo. T.A., Gil-Garcia, J.R., 2009. Information sharing at national borders: Extending the utility of border theory. *42nd Hawaii International Conference on System Sciences,* 1-10.

Ojasalo, J., Turunen, T., & Sihvonen, H., 2009. Responsibility and decision making transfer in public safety and security emergencies - A case study of school shootings. *IEEE Conference on Technologies for Homeland Security*, 358-365.

Pirinen, R., Rajamäki, J. (Eds.), 2010. *Integrative student-centred research and development work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)*. Vantaa: Laurea publications.

Pirinen, R., Rajamäki, J., 2015. Mechanism of Critical and Resilient Digital Services for Design Theory," *2nd International Conference on Computer Science, Computer Engineering & Social Media*, IEEE, 90-95.

Rajamäki, J., 2013. The MOBI Project: Designing the Future Emergency Service Vehicle, *IEEE Vehicular Technology Magazine*, Vol. 8, No. 2, 92-99.

Rajamäki, J., 2014. Software Intensive GNSS-Based Tracking Systems for Improving Law Enforcement, *WSEAS Transactions on Systems and Control*, Vol. 9, 629-639.

Rajamäki, J., 2015. Cyber Security Education as a Tool for Trust-building in Cross-Border Public Protection and Disaster Relief Operations," *IEEE EDUCON Global Engineering Education Conference,* 378-385.

Rajamäki, J., Knuuttila, J., 2013. Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-on-custody Requirement, *European Intelligence and Security Informatics Conference*, 198-203.

Rajamäki, J., Knuuttila, J., Ruoslahti, H., Patama, P., Viitanen, J., 2015. Building Trust between Citizens and Their Governments: A Concept for Transparent Surveillance of Suspects, *2nd International Conference on Computer Science, Computer Engineering & Social Media*, IEEE, 128-133.

Rajamäki, J., Pirinen, R., 2015. Critical Infrastructure Protection: Towards a Design Theory for Resilient Software-Intensive Systems," *European Intelligence and Security Informatics Conference (EISIC)*, IEEE [In Press].

Rajamäki, J., Pirinen, R., Knuuttila, J. (Eds.), 2012. *SATERISK - Risks of Satellite-Based Tracking: Sample of Evidence Series.* Vantaa: Laurea-University of Applied Sciences.

Reivo, J., Vuoripuro, J., Pelkonen, N., 2010. Communication and security man-agement cooperation in large events - Case: IAAF World Chanpionships 2005 in Helsinki. In R. Pirinen & J. Rajamäki (Eds.) *Integrative student-centred research and development work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)*. Vantaa: Laurea Publications, 119-136.

Tikanmäki, I., Rajamäki, J., Pirinen, R. (Eds.), 2014. *Mobile Object Bus Interaction: Designing of Future Emergency Vehicles.* Sample of Evidence Series: Volume (3), Vantaa: Laurea publications.

Tourish, G., Hargie, O., 2004. *Key Issues in Organizational Communication.* Psychology Press.

Yin, R. K., 2009. *Case Study Research Design and Methods*. Thousand Oaks: Sage Publications.