Author(s): Lehto, Martti

Title: Cyber security competencies : cyber security education and research in Finnish universities

Year: 2015

Version:

Please cite the original version:

Lehto, M. (2015). Cyber security competencies : cyber security education and research in Finnish universities. In N. Abouzakhar (Ed.), ECCWS 2015 : Proceedings of the 14th European Conference on Cyber Warfare & Security, University of Hertfordshire, Hatfield, UK, 2-3 July 2015 (pp. 179-188). Academic Conferences and Publishing International Limited. Proceedings of the European conference on cyber warfare and security. http://tinyurl.com/ECCWS2015

Cyber security competencies – cyber security education and research in Finnish universities

Martti Lehto, Faculty of Information Technology, University of Jyväskylä, Finland

martti.lehto@jyu.fi

Abstract: The revolution in information technology that began in the 1990s has been transforming Finland into an information society. Imaginative data processing and utilization, arising from the needs of citizens and the business community, are some of the most important elements in a thriving society. Information and know-how have become key 'commodities' in society, and they can be utilized all the more efficiently through information technology.

Individuals, public and private organizations alike depend on the cyber world. From the citizens using social media, to banks growing their business, to law enforcement supporting national security – every sector of the society is increasingly dependent upon technology and networked systems. While the public sector, the economy and the business community as well as citizens benefit from globally networked services, the digital IT society contains inherent vulnerabilities which may generate security risks to citizens, the business community or the vital functions of society.

Without sufficient awareness of the risks in cyber world, however, behavioral decisions and unseen threats can negatively impact the security of the critical infrastructure and can cause physical damage in the real world. On an individual level, what is at stake is the vulnerability of each individual user in cyber world.

As the world grows more connected through cyber world, a highly skilled cyber security workforce is required to secure, protect, and defend national critical information infrastructure. Across the private and public sector organizations are looking for well-trained professionals to assess, design, develop, and implement cyber security solutions and strategies. While the demand for cyber security professionals is high, the supply is low. Meeting the growing demand for cyber security professionals begins in the education system.

The most efficient custom to increase cyber security is the improvement of the know-how. The cyber security strategies and development plans require the improvement of the know-how of the citizens and actors of the economic life and public administration.

Pursuant to Finland's Cyber Security Strategy (2013) "the implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society".

In this paper are analyzed the know-how demands and needs of the cyber security which the different actors of the cyber world present. The know-how demands and needs are compared with the cyber security research and education which is offered in Finland's universities. The paper is based on a survey conducted on Finnish universities in 2013 and 2014 and on the analysis of its results.

Keywords: cyber strategy, cyber education, cyber competence

1. Introduction

The global cyber world connects states, businesses and citizens in an entirely new manner. The significance of time and place in communications has transformed. Although the digital information society has remarkably increased well-being, on the flip side it also contains risks of various cyber world threats. The target of an attack can be inexpensively reached from anywhere in the world, and the command servers that execute the operation can be positioned in any country, cloaking the actual perpetrator of the attack.

Competence is a crucial point at issue for the information society. In addition to boosting cyber security's qualitative and quantitative competencies new methods, instruments and pedagogical skills are needed, which can both improve the quality of education and increase the appeal of ICT studies and the desire to continue with post-graduate studies. Competence includes attributes such as individuality and a sense of community which are derived from the combined effect of formal education and informal experiences.

The goal of improving cyber security competencies is to boost the skills of citizens and professionals in such a manner that by 2016 Finland will be a global forerunner in cyber threat preparedness and in managing disruptions caused by these threats. This paper analyzes the fundamentals of national cyber security

research and education, defines cyber security competencies and evaluates cyber security research and education at different universities and research institutes.

The research was conducted with universities and research institutes. The methodology used in the research was qualitative and the methods used were interviews and reviewing different kinds of written material. This paper first looks at Finland's education system, then, in chapter 3, at the fundamentals of cyber security research and education. Chapter 4 deals with cyber security as a field of research and chapter 5 discusses it as a field of education. Chapter 6 depicts cyber security research and education in universities and research centers. Finally, the conclusions are presented.

2. Finnish Education System

The Finnish education system is composed of:

- Nine-year basic education (comprehensive school) for the whole age group, preceded by one year of voluntary pre-primary education
- Upper secondary education, comprising general education and vocational education and training (vocational qualifications and further and specialist qualifications)
- Higher education, provided by universities and polytechnics

The Finnish higher education system consists of two complementary sectors: polytechnics and universities. The mission of universities is to conduct scientific research and provide undergraduate and postgraduate education based on it. Universities must promote free research and scientific and artistic education, provide higher education based on research, and educate students to serve their country and humanity. In carrying out this mission, universities must interact with the surrounding society and strengthen the impact of research findings and artistic activities on society. (MEC 2015)

At universities students can study for Bachelor's and Master's degrees and scientific or artistic postgraduate degrees, which are the licentiate and the doctorate degrees. In the two-cycle degree system students first complete the Bachelor's degree, after which they may go for the Master's degree. As a rule, students are admitted to study for the Master's degree. (Ibid.)

3. The Fundamentals of Cyber Security research and education

3.1 Cybersecurity Strategy of the European Union

According to the Cybersecurity Strategy of the European Union EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. The strategy proposes specific actions that can enhance the EU's overall performance. These actions are both short and long term, they include a variety of policy tools and involve different types of actors, be it the EU institutions, Member States or industry. Step up national efforts on network and information security (NIS) education and training, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations. (European Commission, 2013)

3.2 Digital Agenda for Finland 2011-2020

The Digital Agenda for Finland 2011-2020, where the goal is that information resources are widely accessible to the general public so that they promote innovation and research activities, the development of digital products, services and markets, the efficiency, impact and transparency of public administration and citizens' participation in decision-making. (MTC, 2010)

Advances in ICT technology significantly impact the manners in which education, research and culture are generated, relayed and utilized. The increasingly routine e-transactions and the wide use of ICT in all business life require sufficient information society and media skills from the entire population. The rapid transformation of the information society creates a continuous demand for multidiscipline information-society research data. (Ibid.)

3.3 Finland´s Cyber security strategy

According the Finland's cyber security strategy as a small, capable and collaborative country Finland has excellent chances of rising to the vanguard in cyber security. The implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society. Cyber security development will heavily invest in cyber research and development as

well as in education, employment and product development so that Finland can become one of the leading countries in cyber security. The strategic goal 7 states that “Inputs into R&D and education will be increased as well as action to improve cyber security know-how in the whole of society.” (Finland´s Cyber security strategy, 2013)

3.4 The implementation programme for Finland’s Cyber Security Strategy

Pursuant to the implementation programme (sic) for Finland’s Cyber Security Strategy, “Research and education in cyber security, development of technologies and innovations within the sector foster economic growth and national distinctiveness. Research cooperation between the authorities will be strengthened as part of the security research implementation program. Intersectoral research requirements and priorities will be merged into common research themes and projects annually… Even though Finnish companies and research units possess top-level cyber and information security proficiency, their competence is fragmented. In order to improve the breadth of competence, more effort must be put into cooperation between units, institutes and the rest of society.” (Implementation programme for Finland’s Cyber Security Strategy, 2014)

In accordance with the implementation program it is necessary to assemble an overall picture of the present state of cyber competence, and to take action to develop the field’s R&D and innovation capacity. The goal is to determine the situation in cyber security competence and the key sectors of research, and to assess the maturity level with particular attention on promoting university-level information and cyber security education, and R&D. (Ibid.)

3.5 The 2013 report of the ICT 2015 working group

There is a shortage of cyber security professionals in Finland. Hence, from the standpoint of Finland’s future success the ICT 2015 working group identified the following items associated with technological competence: development of in-depth data-processing expertise and ensuring the creation of critical clusters of competence in key technologies (digital services and content, gamification, data security, mobility and big data). Extensive competence is needed in creating internationally competitive and secure ICT-intensive products and services. Success demands that companies have core development teams manned with top-level experts in cyber security technology which comprehensively master the central sectors of their field. (MEE, 2013)

Research and education increasingly link both information management and information-intensive expertise with companies’ competitiveness and with achieving and maintaining a competitive edge. By intensifying research and education in the field, it is possible to accomplish scientific breakthroughs, innovation, technological advances, better productivity and, consequently, national well-being.

3.6 INKA Cyber Security Programme

The Ministry of Employment and the Economy has selected five themes for the Innovative Cities (INKA) programme (sic) (2014-2020), which has been launched in 2014. Jyväskylä is responsible for cyber security. The purpose of the program is to accelerate major projects that create new business and international competitive advantages through cooperation between cities, the state, academia and industry. The INKA security theme enables Finnish expertise to further develop and gain new momentum for economic growth from urban regions.

The vision of the INKA cyber security theme is to make Finland an internationally renowned, global pioneer in cyber security business and competence and in cyber threat preparedness. The aim of the theme is to create a national network of education, research and business, and international activity which helps develop competence and new business in the field. Further aims include the creation of new companies, foreign companies being established in Finland, and the creation of a national cyber security cluster. (INKA, 2014)

4 Cyber security as a field of research

Security and the cyber domain cover several fields of life and research topics. Many scientific disciplines address themes associated with cyber security. Computer science and engineering, information systems science, information processing science, ICT technology as well as system engineering have studied cyber security related questions for a long time already.

A multidisciplinary approach characterizes cyber security research. Cyber security can be approached from the standpoint of using and developing mathematical models through the development of anomaly detection and control. A computational science approach can effectively achieve research results, as different complex systems (technical, human-oriented) can be more accurately modelled and optimized. The use of applied

mathematics or scientific computation in researching progressively complex cyber security phenomena enables solving increasingly difficult problems or society's complex security challenges.

By employing the methods of research used in cognitive science it is possible to combine different research fields in the human sciences and techno-economics. A cognitive science approach makes it possible to study the cyber environment in a problem-oriented and multidisciplinary manner by integrating competence in closely associated sciences in order to solve interdisciplinary questions. The research focuses on creating a reliable and valid model which can determine relevant human performance criteria in a digital environment. The research highlights the mechanisms which affect observation, learning, memory, comprehension, reasoning and interaction. The goal is to try to explain which kind of data representations and data-processing methods in a digital situation picture environment result in optimal and adaptive behavior, especially in exceptional conditions.

Information processing science as a discipline studies problem associated with ICT technology and its use. Cyber security is a cross-cutting theme in the field, extending to a wide range of technologies and processes as networks, computers, programs, data and applications are being protected from cyber-attacks and damage. The justifications for the competence extend to information systems science, ICT technology and information processing technology.

5. Cyber security as a field of education

Cyber security competence is not just another professional field of expertise. Rather, it ranges from civic skills all the way to international-level professions. Therefore, cyber security should be included in different educational levels. When it comes to comprehensive level education, the education must ensure that young people sufficiently have the skills required by the cyber domain, that they understand its threats, and that they can protect themselves accordingly. In the upper-secondary level and vocational education these competencies are further deepened, creating the base for special expertise in higher-level education. Vocational education can include such cyber security education and training which provides basic professional skills and qualifications needed in working life.

Universities emphasize the scientific research of cyber security, and concomitant education. Polytechnics provide practical-oriented cyber security education which corresponds to the needs of employment. It should be possible to receive Bachelor's, Master's and Doctorate degrees in cyber security. Correspondingly, polytechnics should also make it possible to receive Polytechnic Bachelor's and Master's degrees in cyber security. Cyber security education provided across the spectrum of higher education generates top-level experts for the different tiers of society, whose skills and know-how meet the competence requirements determined for each task.

Cyber security must be included as a part of adult education. Such education can include basic degree level education, studies included in a degree, training that prepares for competence-based qualification, apprentice training, supplementary and continued education to update and expand a person's professional skills as well as social studies and leisure studies that improve civic and working skills.

The effective development of national cyber security expertise demands the determination of competence areas and their contents, so as to make it possible for each level of education to provide the needed education. This paper has analyzed the competence areas of cyber security and their contents. Each competence area encompasses several core competencies. On the basis of the contents of the competence areas and core competencies it is possible to determine the required courses which aim at achieving the desired proficiencies. List below illustrates identified cyber security competence areas.

- Cyber security fundamentals
- Operating system security
- Network Security
- Software Security
- Database Security
- Web security
- Anomaly Detection
- Cryptology
- Information Assurance
- Information Security Management

- Secure System Design
- Critical Infrastructure (CIP) and Information Infrastructure Protection (CIIP)
- Cyber warfare and Cyber conflicts
- Cyber Business
- Compliance and Legal Issues
- Digital Forensics
- Human Aspects of Cyber Security

6. Cyber Security Research and Education in Universities and Research Centers

Security and the cyber domain embrace many walks of life and research subjects. A number of disciplines address themes associated with cyber security. For a long time already questions associated with cyber security have been studied in computer science and engineering, information systems science, information processing science, ICT technology as well as automation science and engineering.

Traditionally, universities have dedicated separate departments to information technology, the information processing sciences and to automation science and engineering. In addition to these, research has been intensified in big data, cloud services, usability and embedded systems, among others, which also include perspectives on cyber security.

In support of continuously improving the competence and awareness of the actors of society, inputs will be made to developing, utilizing and training common cyber security and information security instructions. Inputs into R&D and education will be increased as well as action to improve cyber security know-how in the whole of society.

6.1 Aalto University

Aalto University works towards a better world through top-quality research, interdisciplinary collaboration, pioneering education, surpassing traditional boundaries, and enabling renewal. Cyber Security research and education has executed in School of Electrical Engineering and School of Science.

Cyber security research at Aalto University is wide-ranging. The School of Electrical Engineering has extended its research to societal and technical topics. In addition to risk analysis, modelling, security considerations in diverse systems, and questions related to cyber security in public administration, the legislative perspective is also covered.

At Aalto University cyber security is always studied in conjunction with an application schema, rather than as a major subject or program. Although information networks are the key application schema, it is possible to include information security studies as a minor subject along with any field of technology.

The research themes are Network Security, Vulnerability analysis, Intrusion Prevention/Detection System, Cloud technology Security, SCADA Security, Legal aspects in Cyber World, Internet Security, Smart Grid Security, Risk analysis, Cyber competencies in public sector

6.2 University of Helsinki

The University of Helsinki is the most comprehensive research institution of higher education, edification and intellectual regeneration in Finland. Precise reasoning is one of the focus areas. This focus area encompasses mathematics and information sciences as well as their applications in other fields.

In the Faculty of Science (Department of Computer Science and Department of Physics) the cyber security research themes are Secure Systems, Mobile Security, Trust Management, Data Security and Usability, Internet of Things, Network Protocols, Big Data, Security of the Distributed Systems, ICT- applications and Cryptology.

Faculty of Science themes of the cyber security advanced studies (80 ECTS) are Information Security, Cryptography and Network Security, Software Security, and Mobile Platform Security.

6.3 University of Jyväskylä

The University of Jyväskylä is a nationally and internationally significant research university and an expert on education that focuses on human and natural sciences. The University is Finland’s leading expert in teacher education and adult education, as well as the major exporter of education. One main technology focus area is Human-centered information and communication technology.

The Faculty of Information Technology responds to the challenges in research and education brought by the development of information technology and digitalization. The Faculty holistically integrates the perspectives of technology, information, organizations, business and people in its research and education.

Information Security the Master of Science education (120 ECTS) is based on two sub-programs: technology profile and organization security profile. The aim of the Master's Degree Program in Cyber Security is to provide solid skills in the kinds of demanding management and development tasks that require comprehensive awareness in cyber security. The studies comprise an entity which addresses the cyber world and its security from societal, functional, systemic and technological perspectives.

The Cyber Security Research areas are anomaly detection, advanced persistent threat (APT), Big Data Security, Cyber Defence, Critical infrastructure protection, Cyber Security and Human aspects, Cyber Security Investments, Cyber Security Management, Cyber Security situation awareness, Identity protection, Secure services, Security economics, social engineering and phishing.

6.4 National Defence University

The National Defence University is a training institution responsible for educating the future leaders of Finland's armed forces. The National Defence University offers undergraduate, masters and doctorate studies and research programs in the area of military science.

Military science is a multidisciplinary and complex collection of subjects that study wars, crises, other threats to security and means for preventing these. In today's world, military science must comprehend military security and defense from a wide security framework perspective. At the National Defence University, the main research interest is above all future threat scenarios and the development of the national defense system.

Different departments of the National Defence University engage in cyber security research. The Departments of Strategic and Defence Studies, Leadership and Military Pedagogy as well as Tactics and Operations Art bring different approaches to the field of research. The Department of Military Technology especially studies the possibilities of compiling a situation picture of critical infrastructure.

6.5 University of Oulu

The University of Oulu is a multidisciplinary science university with international operations. The university operates in eight major fields: Humanities, Education, Economics, Natural Sciences, Technology (incl. Architecture), Medicine, Dentistry and Health Care, distributed in six faculties. Focus areas of the university are: Biosciences and health, Information technology, Cultural identity and interaction, Environment, natural resources and materials.

Research on information security at the Department of Information Processing Science at Oulu University's Faculty of Information Technology and Electrical Engineering concentrates on research areas such as secure coding, digital watermarking and biometric identification.

The Department of Computer Science and Engineering runs an associated degree program, which includes information security studies. The degree program at the Department of Information Processing Science also includes information security studies. Cryptography and encryption techniques can be studied at the Department of Mathematical Sciences.

6.6 Tampere University of Technology

Tampere University of Technology is primarily a research university, which specializes in technology and architecture. Technology is the key to addressing global challenges. The University combines a strong tradition of research in the fields of natural sciences and engineering with research related to industry and business.

The Cyber Security Research areas are Cloud Computing Security, Identity and Access Management, Key Management, Cryptographic Protocols, Secure Programming, SCADA Security.
The syllabus for information security, studied as a minor subject, includes programs, network, management and cryptology. The Department of Automation Science and Engineering has integrated information security into its basic studies of systems, and automation into the studies of information systems. The cyber security approach has set out from the following perspective: "information security, communications technology,

software technology and the methods of software engineering are tools used in generating reliable automation".

6.7 University of Turku

The University of Turku is an internationally competitive university, the operation of which is based on high-quality multidisciplinary research. High-level research creates the base for the university. The Strategy of the University of Turku has identified information security as one of four research areas that are in an advanced stage of development. Turku University provides a multidisciplinary research environment in information security, bringing together experts in information technology, mathematical cryptography and information systems science.

Research topics include *inter alia* cryptology, information security and data protection in mobile communications, software security, security in embedded systems, network security, and human aspects of information security as well as information security and guaranteeing business continuity management.

Master's Degree Program in Information Security and Cryptography (120 ECTS) has two tracks: Cryptography and Data Security, and Networked Systems Security. The Cryptography and Data Security major subject educates future experts of the field that have strong and broad knowledge on mathematical aspects of cryptography and data security. The students learn to assess the strengths and weaknesses of cryptographic solutions based on a deep understanding of the underlying theory. The Networked Systems Security major subject gives its students profound and substantial education and expertise in the networked systems security and technology field.

6.8 Technical Research Centre of Finland

Technical Research Centre of Finland (VTT) is a globally networked multi-technological applied research organization. VTT provides high-end technology solutions and innovation services. Research activities at VTT encompass forecasting future technological and market development trends, creating novel know-how, providing customers with new development impulses, developing technologies and concepts, applying technologies, and enhancing technology transfer and utilization.

VTT focuses its research spearheads on specific areas, which will be undergoing major business transitions or radical technology changes. VTT's research vision is directed by two major trends: digitalization and sustainable development. Information digitalization guides not only information and communication technology, but also the development of all its application areas. Sustainable development, on the other hand, requires taking environmental aspects into account in products and services as well as production processes.

VTT Technical Research Centre of Finland studies and develops suitable methods for the purpose of sustaining information security in software-intensive systems and products and serving the needs of the ICT industry. The main research topics in this field are: information security analysis methods, securing software security, monitoring and guaranteeing information security in operational systems, and information security metrics.

6.9 Finnish Defence Research Agency

The Finnish Defence Research Agency (FDRA) is a military institution under the authority of Defence Command Finland and provides advanced research, development, testing and evaluation services for the Finnish Defence Forces. Defence Research Agency is a multidisciplinary research and development organization bringing together research and development activities related to military, behavioral, social and natural sciences under one roof.

The Electronics and Information Technology Division focuses on research of electronic defense applications. Division researches Radiofrequency Sensor and Electronic Warfare Systems, Cyber Defence and C4-Systems. Main Cyber Defence research areas are vulnerabilities and cryptology.

7. Summary and discussion

The EU and Finland alike have set requirements for improving national cyber security competencies. The EU expects that network and information security (NIS) education be provided in schools and universities, and that supplementary training be given within the public administration.

The Digital Agenda for Finland 2011–2020 maintains that IT skills, communication skills, media literacy and the use of social media constitute the foundation for the skills needed to use digital services. The proposed goals included the incorporation of ICT use as an integral part of the education in schools as well as in basic and supplementary teacher training. In addition, the investment in applied ICT know-how should be scaled up – with cyber security being one of its elements – and given a more prominent place in curriculum design throughout all tertiary education.

The implementation programme for Finland's Cyber Security Strategy puts forward that "universities shall bolster the preconditions of cyber security's basic and applied research and innovation at the national and international level".

The ICT 2015 working group states that "extensive competence is needed in creating internationally competitive and secure ICT-intensive products and services.

The INKA project defines cyber security education as a spearhead theme, according to which the development of Masters and post-graduate programs in cyber security is continued by expanding and intensifying the availability of courses and studies, by creating a national network of expertise to provide top-level education.

Cyber security education is on the rise in Finland. The aforementioned goals have been the foundation on which Finnish universities have developed their cyber security research. Two models of education are being used: a curriculum that focuses on cyber security or one that integrates cyber security studies into other curricula. The previous model is used by the Jyväskylä and Turku Universities and the latter, integrated approach, by other universities. Both models are indispensable for improving competence in the field. The cyber security curriculum generates experts in the domain of cyber security who have become adept in some niche area. The integrated approach generates experts who master a specific field of technology (ICT technology, communications technology, automation science, etc.) as well as attendant cyber security issues.

The challenge regarding the way things are now is the lack of cyber security education objectives for the entire education system. The sought-after improvement of competencies requires defining the basic skills and competencies for the entire national education system. It is necessary to have an understanding of what each citizen needs to know about cyber security, the demands of working life, what kind of professional skills are needed and what kind of supplementary training needs to be provided to those already in working life. At the moment universities only provide cyber security education from their own perspectives without a clear vision of national cyber security competencies.

The national research co-operation of the academic ecosystem has efficient forms of cooperation involving cyber security in the operational practice of Internet Service Providers (ISP), corporate and other networks. Finland has good research infrastructure supporting cyber security research and collaboration. There is a large number of cyber security laboratories in Finland. These laboratories allow research into and experimenting with cyber security threats and infrastructures without the restrictions of the public Internet. The national cyber security research creates methods and tools for fast, accurate, robust and privacy preserving forms of cooperation among the networked entities towards the goal of better cyber security and the capability of effectively responding to threats, even at the national security level. (Digile 2014)

In order to improve the present situation the Prime Minister's Office launched a research program aimed at generating information by the end of 2015 on advancing national cyber security education and R&D&I activities. This research is also seeking to establish an international dimension which would enhance the improvement of Finland's cyber security competencies.

While the recently completed cyber security competency survey demonstrates that both national and international requirements have been implemented throughout Finnish universities, a clear national vision of the required skills and competencies is still missing. Even though cyber security research is prolific in different universities, thus far no cyber security research profiles have been determined at the national level. In order to make cyber security research world class, Finland must have the ability to identify nationally important research areas and establish sufficient resources for them. The research highlights cooperation between universities, both national and international.

References

Digile (2014), Strategic Research Agenda for Cyber Trust, 12.6.2014

European Commission (2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013

INKA (2014) Innovative Cities programme 2014–2020, cyber security theme, implementation programme v2.1, 1.2.2014

The implementation programme for Finland's Cyber Security Strategy (2014), the Security Committee, 11 March 2014 http://www.turvallisuuskomitea.fi/index.php/en/kyberturvallisuusstrategia/toimeenpano-ohjelma

Ministry of Education and Culture, MEC (2015), Education System in Finland, http://www.minedu.fi/OPM/Koulutus/koulutusjaerjestelmae/?lang=en

Ministry of Employment and the Economy, MEE (2013), 21 paths to a Frictionless Finland, Report of the ICT 2015 Working Group, 18/2013

Ministry of Transport and Communication, MTC (2010), Productive and innovative Finland – digital agenda for the years 2011-2020. http://www.lvm.fi/pressreleases/1212700/increased-productivity-through-development-of-information-society

Finland's Cyber Security Strategy (2013). Government Resolution 24 January 2013, http://www.yhteiskunnanturvallisuus.fi/en/materials

Appendix 1: Cyber Security Research areas in Finnish Universities

	Aalto Univ.	Univ. of Helsinki	Univ. of Jyväskylä	Defence Univ. and FDRA	Univ. of Oulu	Tampere Technical Univ.	Univ. of Turku	VTT
Anomaly detection			X					X
APT analyze			X					X
Authentication, authorization &identity management (IAM)						X		X
Big Data Security	X		X					
Cloud service security	X				X	X		X
Computer Security	X		X		X			
Cryptography	X	X		X	X	X	X	X
Cyber Defence			X	X				
Cyber Security legal aspects	X							
Critical infrastructure protection	X		X	X		X		X
Cyber Security and Human aspects			X		X		X	
Cyber Security Investments			X					
Cyber Security Management			X					
Cyber Security situation awareness	X		X	X				X
Data mining and analysis and Cyber Security		X	X					
Dos/DDos attack protection	X		X					
Incident analysis and management								X
Identity and access management	X					X		
Identity protection			X					
Industrial Control System (ICS) security	X				X			X
Information Assurance		X						X
Information Security		X	X		X	X		
Intrusion detection	X		X					X
Intrusion Prevention	X		X					
IoT security	X	X	X		X	X		X
Machine learning methods for Cyber analysis			X					
Mobile security	X	X	X			X	X	
Network security	X	X	X			X	X	

and monitoring								
Privacy	X							X
Risk analyze	X							X
SCADA security	X		X	X		X		X
Secure services			X				X	X
Secure System Design	X		X		X	X		
Security architectures and communication protocols	X	X			X			X
Security economics			X				X	X
Security information visualization and interpretation			X	X				X
Security metrics and data aggregation			X					X
Security standardization								X
Security testing			X		X			X
Smart Grid Security	X					X		X
Software Security		X	X		X		X	
Systems Security	X	X			X	X	X	
Threat, vulnerability and dependency analysis	X		X	X			X	X
Trust management	X	X	X			X		X