Limnéll, Jarno; Lehto, Martti

The importance of strategic leadership in cyber security

Published in:
Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019

Published: 01/01/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Limnéll, J., & Lehto, M. (2019). The importance of strategic leadership in cyber security: Case of Finland. In T. Cruz, & P. Simoes (Eds.), *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019* (pp. 288-296). (Proceedings of the European conference on cyber warfare and security; Vol. 2019-July). Academic Conferences and Publishing International.

The Importance of Strategic Leadership in Cyber Security: Case of Finland

Jarno Limnéll[1] and Martti Lehto[2]
[1]Aalto University, Finland
[2]University of Jyväskylä, Finland
jarno.limnell@aalto.fi
martti.j.lehto@jyu.fi

Abstract: Cyber security has become one of the biggest priorities for businesses and governments. Streamlining and strengthening strategic leadership are key aspects in making sure the cyber security vision is achieved. The strategic leadership of cyber security implies identifying and setting goals based on the protection of the digital operating environment. Furthermore, it implies coordinating actions and preparedness as well as managing extensive disruptions. The aim of this paper is to define what is strategic leadership of cyber security and how it is implemented as part of the comprehensive security model in Finland. The paper also asks (and answers) how the strategic leadership of cyber security must be organised. This paper provides proposals for managing strategic cyber security in society and public administration, for managing large disruptions in the cyber operating environment. Key data consists of different security-related strategies and instructions, existing research information, and interviews with public sector actors and experts of the field. In terms of effective strategic leadership of cyber security, it is vital to identify structures that can respond to the operative requirements set by the environment. As a basis for national development and preparedness, it is necessary to have a clear strategy level leadership model and situation awareness that supports management. They are also necessary for the management of serious, extensive disruptions in both normal and exceptional conditions of the cyber operating environment. The challenges of cyber security management are particularly prominent at the level of strategic leadership. In order to ensure cyber security and achieve the set strategic goals, society must be able to engage different parties and reconcile resources and courses of action as efficiently as possible. Cyber capability must be developed in the entire society, which calls for strategic coordination, management and executive capability. The goals presented in Finland's Cyber Security Strategy have guided the creation of strategic leadership models for cyber security. Alternative models for the strategic leadership of cyber security in Finland is presented in the paper.

Keywords: cyber security, strategic leadership, situational picture, leadership, national security

1. Introduction

1.1 Background

Cyber security is an elemental part of society's comprehensive security, and the cyber security operating model is in keeping with the principles and practices specified in Finland´s Security Strategy for Society (2017).

Technical and economic development has led to networking and increasing interdependencies between production, services and entire society. An efficient and optimised network economy is based on rapidly developing information and communication technology, which is vulnerable to many new types of threats and risks. Cyber-attacks, malware, denial of service attacks and different forms of influencing through information are becoming ever more prolific. The reliable operation of telecommunications, information systems and communications are an essential precondition for modern society's undisrupted functioning, security and citizens' livelihoods. This is also about maintaining citizens' trust in a well-functioning society. The development of business continuity management accounts for a large proportion of the security of supply work carried out in the information society sector. Due to this development, improved preparedness for maintaining the functioning of society's vital information technology systems and structures in the face of cyber threats and incidents is also needed in normal conditions. In particular, it should be noted that Finnish society's and companies' dependence on the cyber environment will grow further in the years to come. (Lehto et al., 2018)

A strategic level leadership model and situational awareness is needed to create the foundation for national preparedness as well as for the leadership of cyber domain – for both in normal time conditions and during emergency conditions. The weakness of the current model is notified in several researches (Lehto et al., 2017). In the cyber environment, strategic sensitivity requires an ability for forming a situational picture and creating situational awareness rapidly for the basis of decisions and actions. Preconditions for building an environment

for cyber security situational picture are shared situational awareness, coordinated and networked management and sufficient expertise in different areas of cyber security.

The national strategic leadership of cyber security consists of two entities: managing cyber security preparedness and managing serious and extensive incidents in normal and emergency conditions.

1.2 Objectives

This research paper prepared proposals for measures related to the management of society's and public administration's cyber security and managing extensive disruptions in the cyber environment. Key research questions examined were the following:

- What is strategic leadership of cyber security?
- How is strategic cyber security leadership implemented in the responsibility model for comprehensive security?
- How should the strategic leadership of cyber security be organised?

1.3 Data and methodology

Highly versatile and extensive material was collected for this study. Key data consisted of different security-related strategies and instructions, existing research information, and interviews with public sector actors and experts of the field[1]. The research project interviewed 40 employees in managerial roles and officers responsible for information/cyber security in private and public organisations. The interviews were conducted in 25 key organizations. Based on the interviews, document analysis and international comparison data, an analysed data set was created, on which the observations, proposals and models presented in this study are based.

Finland's Cyber Security Strategy and its background dossier (Security committee, 2013) and its Implementation Programme 2017-2020 (Security committee, 2017a), the Security Strategy for Society (Security committee, 2017b), a report titled Central Government Communications in Incidents and Emergencies (Prime Minister's Office, 2013), the Guidelines for developing Finnish legislation on conducting intelligence – A report of the Working Group (Ministry of Defence, 2015) and the National Audit Office's performance audit report titled Cyber Protection Arrangements (National Audit Office, 2017) were used in the research project. Key documents also included other central government strategies like Information Security Strategy for Finland (Ministry of Transport and Communications, 2016) and others.

2. Strategic leadership of cyber security

2.1 Definitions of strategic leadership of cyber security

It must be noted that strategic leadership is not an unambiguous term (Juuti & Luoma 2009). It may be defined and understood in many ways. Additionally, the "boundaries" between strategic and operative management are not always clear in all situations of cyber security management, and in some instances, they are difficult to separate (while this may even be unnecessary). Different definitions of strategic leadership and the difficulty of separating strategic and operative activities also emerged, among other things, in the context of the interviews conducted for this study and the reference countries selected for the international comparison. For example, strategic leadership of cyber security was described as follows in the interviews: "Strategic leadership means leading a phenomenon at the highest level, making an effort to define long-term visions and objectives as comprehensively as possible".

Cyber security is an aspect of society's and companies' security, which is highly important when considering an organisation's strategic goals in an increasingly digital society. In the source documents of the study, strategic leadership of cyber security was often described as securing the central government's capabilities and vital

[1] The interviewees represented the following organisations: CGI Finland Oy, Confederation of Finnish Industries, Elisa Corporation, F-Secure Oyj, Fingrid Oyj, Finnish Information Security Cluster, National Emergency Supply Agency, Emergency Response Centre Administration, Insta Group Oyj, National Bureau of Investigation, Ministry of Transport and Communications, National Police Board, Ministry of Defence, Finnish Defence Forces, Ministry of the Interior, SSH Communications Security Oyj, State Security Networks Group, Finnish Technology Industries, Tieto Corporation, Security Committee, Prime Minister's Office, Government ICT Centre Valtori, Ministry of Finance, Finnish Communications Regulatory Authority (incl. Nation-al Cyber Security Centre Finland), and Ministry for Foreign Affairs.

functions, also allowing the private and the NGO (non-governmental organisation) to build their activities on well-functioning and secure information networks. Based on these documents, the most important task of the strategic leadership of cyber security is defined as creating a vision and a national mentality which are recognised at all levels of actors participating in cyber security work and which direct the actions in both normal and emergency situations. (Lehto & Limnéll, 2016).

Strategic leadership comprises *long-term implementation* of Finland's Cyber Security Strategy (2013) and Finnish cyber security. Strategic leadership brings society towards the selected vision. The task of implementing strategic leadership is based *on identifying and setting objectives* derived from securing the digital operating environment.

Secondly, strategic leadership *reconciles, coordinates and ensures participation in cooperation between different actors* in cyber security activities and preparedness. As cyber security is an extensive societal phenomenon which connects a great number of different actors, the coordination of cooperation is stressed both in normal and emergency conditions and during incidents. Sufficient preconditions for making decisions and clearly defined powers are stressed in the activities.

Thirdly, as cyber security is a strategic issue for Finnish society, the strategic leadership of cyber security takes place in close *interaction with both political decision-making and operative activities.* Strategic leadership is also associated with *strengthening Finland's cyber security identity*, both nationally and internationally. The cyber security identity is also associated with *seeing to national cyber self-sufficiency* regarding both product and service solutions and expertise and research in Finland. Domestic and international *communications play an important role* in creating a Finnish cyber security identity and credibility based on trust. Several international indicators are specifically geared to measuring cyber security identity and capability. One of the goals of strategic leadership thus is the continuous monitoring of the status of national cyber capability (as a whole) to understand its current level and to *improve the capability.*

Fourthly, strategic leadership *creates coherence and continuity* for Finland's collaborative efforts at both the national and international level. Strategic leadership gathers all available resources together in order to *achieve the set targets.*

To sum up: *The strategic leadership of cyber security comprises identifying and setting objectives derived from securing the digital operating environment, coordinating activities and preparedness, and extensive leadership in incident management.*

2.2 Strategic leadership of cyber security – a current status analysis based on research

The challenges of cyber security management are particularly prominent at the level of strategic leadership. The challenges of the current state are reflected in the views brought up in several of the interviews conducted for the study concerning (1) clear and concrete proposals for strategic leadership structures of cyber security, and (2) the need to discuss the importance of this issue and the required measures with integrity and avoiding any ambiguity. Two basic problems have been identified at the level of strategic leadership:

1) The number of actors is large, and for this reason, the strategic leadership of cyber security is fragmented and lacks clear leadership. The ministries carry out the strategic leadership of cyber security independently in their own sectors, and consequently overall strategic leadership is lacking, and the activities are to a great extent siloed in the various administrative branches.

2) No effective cooperation structure exists at the level of strategic leadership of cyber security. This is partly linked to the first problem. The ministries look at cyber security on the basis of their own needs, losing sight of the wider societal perspective, and the aforementioned objectives defined for strategic leadership are not achieved.

The interviews conducted for the study indicate that the strategic leadership of cyber security must be recognisable to avoid a situation where administrative branches have no leadership and the requisite measures cannot be carried out. In the current situation, strategic leadership is expected to take care of itself, even if this is not necessarily the case. In the current state, interdependencies between different actors in society have not

been described. Once the relationships between organisations and functions have been described, the impacts decisions will have on societal functions can be anticipated. Experts believe that research to study the interdependences is needed as soon as possible. Identifying the cooperation partners, actors producing information and the entire cyber observation system would be important first steps towards a genuine cross-cutting security strategy for entire society. The interviews conducted for the study indicate that discretion will be needed concerning a body/function that takes care of coordination across organisational boundaries to ensure that its actual role does not remain illusory and that it does not add to the workload unnecessarily.

In a prior study, a need to centralise the management of Finnish cyber security to the Prime Minister's Office emerged, in particular (Lehto et al. 2017). According to the experts interviewed for the study, due to its direct dialogical connections and role as a function supporting top-level government, the Prime Minister's Office is better placed to assume strategic leadership than other branches of government or organisations. The present model is also linked to EU level cyber security models that the Prime Minister's Office reconciles with national models. The cyber security work at the Prime Minister's Office has close links to the Government's work in this area. The Government serves all branches of administration equally and coordinates their cooperation. Models and practices planned for the Prime Minister's Office are relatively similar to those planned for the Government. However, the Prime Minister's Office has no direct authority over the different ministries, and proposed measures are thus implemented through advice and instructions. According to the interviewees, the present model does not respond fast enough to incidents. The National Audit Office (2017) recommends that "the Ministry of Finance define and implement an operative management model for extensive cyber incidents regarding government ICT services".

In terms of effective strategic leadership of cyber security, it is vital to identify structures that can respond to the operative requirements set by the environment. Typical features of the cyber environment are an accelerating rate of change, a phenomenon-based approach, complexity and, in part, unpredictability. The interviewees stressed that the pre-sent model of strategic leadership is unable to respond to the ever-faster rate of change. The loop formed by gathering information on which decisions are based, making the decision and implementing it is currently too slow. "As the vulnerability of society increases it is necessary to be able to rapidly start managing sudden disturbances in the cyber domain".

According to the majority of experts interviewed for the study, a precondition for the current role of the Prime Minister's Office is that existing forms and practices of cooperation for responding to an urgent crisis in the cyber environment have been negotiated. It is almost never possible to negotiate on measures in urgent crisis situations, and a mandate and operating models tested as part of the preparedness process should exist for taking action. The Finnish Communications Regulatory Authority's National Cyber Security Centre has established methods for managing incidents together with private sector actors. Rather than on authority, this procedure is based on cooperation, in which the Cyber Security Centre serves as the contact point.

The interviews conducted for the study indicate that strategic leadership is based on building and maintaining trust. Even today, deep trust and doing things together are the basis for thwarting cyber threats. Fundamental trust has enabled exceptionally good cooperation between different actors in Finnish society, and this cooperation has long traditions in Finland. The National Cyber Security Centre is a good example of how trust achieves more than obligation. So far, keeping the cyber environment safe has been based on identifying key actors and conducting negotiations between them, rather than cyber security management structures. The interviewees even questioned the strategic leadership of cyber security due to factors stemming from the operating environment. A systematic action model, but the issue of the strategic leadership of government cyber security was found challenging.

According to the experts interviewed for the study, *a strategic leadership model of cyber security should be created, as currently there is no strategic leadership of cyber security.*

2.3 Strategic leadership of cyber security in the future

New technologies challenge the current legislation and raise ethical questions concerning such issues as cyberattack capability, autonomous vehicles, artificial intelligence and augmented reality. The advancing technologies mean that the cyber environment is in constant flux which, according to the interviewed experts, hampers the creation of permanent and straightforward operating models. Diversification of activities, group

processes and a correct type of balance between the mechanical and organic nature of activities are means for managing this complexity.

Based on the interviews, research literature and an analysis of the reference countries, successful strategic leadership of cyber security requires:

- Effective legislation,
- Sufficient powers,
- Links to political decision-making,
- Capabilities and expertise, and
- Financial resources.

The interviewees identified leadership capability as a success factor in the strategic leadership of cyber security. The experts referred to historical cases where decisions were made on the wrong grounds without understanding their impacts on our society. Strategic leader-ship should facilitate interaction between the state's political leadership and, on the other hand, those responsible for operative activities, ensuring that both parties understand each other and that their actions are coherent. According to the experts, one perspective to leadership is that the highest level in the national management of cyber security, or strategic leadership, should be assigned to a ministry that has genuine capabilities for leading the activities.

3. Situational awareness as part of strategic leadership

3.1 Challenges of the current state

The situational picture of the cyber environment is fragmented, and any understanding of it as a whole is based on information shared between the authorities, the private sector, researchers and experts. The interviewees expressed differing views of cyber security situational awareness. Some found the national cyber security situational awareness fragmented and incomplete. A situational picture that would cover all national cyber environment actors is not being put together and analysed, and capability for making decisions is lacking. Lack of powers prevents the creation of efficient observation capability and thus a cyber security situational picture needed for effective management. While different actors have systems built for their own use, shared national situational awareness that could be used both at the strategic and operative level is lacking. Some of the interviewees felt that the situational picture was good, or at least sufficient, in general terms. The current operating model is sufficient for managing minor cyber-attacks, but situational awareness and understanding are inadequate for thwarting complex and extensive attacks. (Lehto et al. 2017)

The structure for maintaining situational awareness was improved as the strategy was formulated, but it continues to have shortcomings at the practical level. Some of the interviewees felt that shared situational awareness is not implemented at the level of ministries. While the administrative branches do not necessarily have an idea of cyber security in society as a whole, they have a relatively good understanding of it in their own sectors. The interviewees also found that exchanges of information partly take place between specific persons. On the other hand, as yet unresolved questions are associated with maintaining a shared situational picture, including who needs what information, on what cycle it is needed, and what type of information is required. Regarding the nature of information, more analysed information on threats as well as unrealised and actual incidents together with solution models for them are called for. From the perspective of improving cyber security preparedness, we must be able to trust that information will flow during incidents and that the actors will know how to respond to it as indicated by their duties. (Lehto et al. 2017)

While there would also be a demand for a sector-specific situational picture service, the National Cyber Security Centre is not currently able to meet it in all respects. Capability for extensively recognising the impacts of incidents should be developed in other sectors of society besides the one specifically affected by the incident. The Cyber Security Centre needs additional resources for developing sectoral situational awareness data and situational picture reserves.

3.2 Analysis of the current state of cyber security situational picture, awareness and understanding

The different parties involved in developing national situational awareness should be able to improve their operations through more effective technical methods, strengthen network-based operation and focus on utilising technical methods in shared use.

The most significant organisations associated with the functional capacity of Finnish society have developed a relatively good ability to observe the situational picture for the part of technical capabilities. Their ability to do so is also improved by networking within their sectors and partly also more extensively, which is supported by good cooperation between the authorities and the private sector. The significance of situational awareness shaped by different organisations' situational pictures (situational picture and its analysis) for the management of entire national cyber security is crucial.

Research has stressed the organisations' possibilities of drawing on different networks for cyber security situational awareness as a national strength, which has also been referred to in previous reports. At least three types of networks relevant to exchanging confidential information can be identified, and they are used actively. They have emerged in connection with business activities, or a specific trust network has been set up between companies in a sector, which may also extend to international cooperation. Additionally, a national trust network between the authorities and the private sector is in place (PPP cooperation).

The response to national incidents consists of the techniques used by different organisations, procedures developed for responding to incidents, and the observation data of different trust networks. This fragmented ability to observe the organisation-specific situational picture and the data reserves it entails could also be used in the analysis phase of large-scale incident management. Preconditions for this arrangement would include the creation of joint operating models and an arrangement based on voluntary exchange of information. A joint data warehouse would enable the further processing of information to analyse a large-scale incident. The required analysis capabilities could be implemented as a network (virtual analysis).

4. Models for the strategic leadership of cyber security and situational awareness

Alternative models for the strategic leadership of cyber security in Finland were produced in the study. The five models presented below are based on the views of personnel with managerial roles and experts of the field in the interviews conducted for the study, international evaluations of reference countries, views presented in the research literature/documents as well as assessments made by the authors.

Five models for the strategic leadership of cyber security are presented:

- 1. The present model
- 2. A national cyber security manager
- 3. A national cyber security unit
- 4. A strengthened National Cyber Security Centre
- 5. A Cyber Security Agency.

4.1 Present model

In the present model, cyber security is managed as part of seeing society's vital functions, and no separate strategic leadership or management process is created for it.

The strengths of this model include its familiarity (management of cyber security is integrated in existing arrangements for incident management) and minor need for rearrangements in the administration. The Finnish (cyber) security actors are relatively familiar with each other, which facilitates information exchanges and smooth cooperation, even if no unambiguous line of command related to cyber security has been defined. This model is underpinned by the current legislation.

The model's weakness lies in its uncertain ability to respond sufficiently fast to large-scale cyber-attacks or incidents and to produce anticipatory strategic analysis data essential for preparing for ever changing cyber

threats. The present management structure cannot be considered optimal in terms of the coordination of preparedness, identification of strategic goals or strengthening of the national cyber security identity. The present model does not provide sufficient guidance for the cyber security preparedness of the administrative sectors, businesses and the NGO, or produce sufficiently centralised capabilities for strategic analysis to support the production of situational awareness. In the present model, shortcomings are associated with the identification and development of national cyber self-sufficiency. No close link between political decision-making and strategic leadership of cyber security, which was stressed in international comparisons, is manifested clearly.

4.2 A national cyber security director

In this model, the role of the top director of cyber security is set up in the Prime Minister's Office or, alternatively, a ministry or an organisation with a key role in cyber security.

A key strength of this model is a clear chain of command in cyber security work: the ap-pointed cyber security manager would coordinate, lead or support cyber security work in all situations. Management would also take place close to political decision-making and steering. In this model, however, a single person would be appointed to direct an area with no dedicated resource allocation.

In this situation, management across administrative boundaries would be challenging, as resource allocations and management systems would be specific to each administrative sector. As another weakness of the model may be considered the concentration of disproportionately great power and responsibility to a single person. As strategic leadership com-prises an extensive set of tasks, the possibilities of a single person carrying out all the specified tasks may be questioned. If the cyber security manager's role is limited to loose coordination, the management of both preparedness and incident response will remain cursory. In a rapidly escalating incident, fast and effective links should be in place between the strategic leadership and operative actors, and each party should have clear-cut powers.

4.3 A national cyber security unit

The model of a national cyber security unit is similar to the national cyber manager model. A separate cyber security unit subordinate to the cyber security manager would be set up with capabilities for directing, developing and supporting national cyber preparedness and for promoting the realisation of the national cyber security vision in a broader sense.

The strengths of the cyber security unit would include its placement close to political decision-making and its ability to direct and develop cyber security activities cross-administratively. From the point of view of management, this can be considered a relatively agile and centralised model, in which the manager is supported by his or her own unit in per-forming a large range of tasks. In reference countries, corresponding units are placed either in the prime minister's office or the ministry with general responsibility for security and jus-tice, or similar tasks are handled by the organisation that has the overall responsibility for the coordination of national security activities. In this model, the management of cyber security is partly integrated with existing arrangements for incident management, and transition to it would thus result in limited needs to rearrange the administration. This would reduce the workload and ambiguities created by changing the arrangements for comprehensive security.

4.4 A strengthened cyber security centre

In this model, the National Cyber Security Centre would be placed under the steering of a cyber security manager, and its operative competence and powers would be complemented with capabilities for strategic analysis. The Centre's situational picture function would be reinforced with strategic analysis capabilities with the aim of producing situational awareness in support of strategic decision-making. The Centre would be co-located with the cyber security manager, and it would work in close cooperation with the Government's Situation Centre. The Situation Centre would continue to perform the task of providing a situation-al picture for the entire Government and all administrative sectors.

The strengths of this model include the proximity of strategic and operative actions, a clear line of command and a straightforward approach, which would translate as agility in deploying capabilities, thus serving the

maintenance of strategic stability while enabling action in unexpected situations. Transition to this model would require limited changes to existing comprehensive security arrangements, including more specific arrangements for cross-administrative cooperation as the Cyber Security Centre takes on its new role. Significant additional resources would also have to be allocated to the Cyber Security Centre.

The weaknesses of this model would include a fragmentation of cyber security functions and the fact that various functions would remain in different administrative sectors. It is also likely to take time before the Cyber Security Centre's reference groups (current and future ones) adapt to its new role.

4.5 A cyber security agency

This model is based on setting up a Cyber Security Agency, which would handle the strategic leadership of cyber security and cyber security functions.

In the agency model, key cyber resources of the central government can be combined into an effective whole, through which the efficiency of both cross-administrative cooperation and collaboration with businesses can be improved. This model would provide an improved ability to respond to changes in customer needs and the operating environment, develop and strengthen the strategic steering of cyber security, and obtain synergy benefits. It can also improve the productivity and, more particularly, the impact of the administration through more diverse and effective resource use.

The weakness of this model is the partial transfer of cyber security functions away from the administrative sectors, with the resulting losses of knowledge of and expertise in the sectors' special features. To create the Agency, broad-based reforms of the existing administrative structures, modifications to the line of command and responsibilities, and adequate resource allocation would be needed. Administrative friction would undermine the efficiency of the activities during a transition period until the new operating model becomes established.

5. Conclusion

In this study, the management models proposed by the research project have been described at the level of principle. Research questions were answered, but the continued preparation of one of the presented leadership models or some other model will require drafting by public servants. In this case, the requisite operative and organisational changes and legislative amendments should be investigated, financial reviews should be carried out, and an extensive assessment of the impacts including statements and a schedule for implementing the reform should be prepared.

The proposed models contain risks, the number and impacts of which are comparative to the scale of the change. The risks may lead to inappropriate solutions when arranging the operations. Consequently, in any further drafting particular attention should be paid to ensuring the quality, reliability and undisrupted continuation of the activities and service level during the potential change and following it.

In order to develop the situational picture, awareness and understanding needed for strategic leadership, the efficiency of the current operating model should be improved, and the data warehouse and cooperation network should be developed. Centralisation of strategic leadership also results in more efficient situational awareness and understanding. The following characteristics, among other things, affect the impact of management: consistency of action in different situations, prevention of siloed activities, taking interdependencies into account, and coordination of activities. The bottlenecks of situational awareness and strategic leadership activities have frequently been identified in expert assessments provided for research projects, and centralisation can thus help optimise limited resources.

References

Juuti P., Luoma M. (2009). Strateginen johtaminen, Kustannusyhtiö Otava, Keuruu 2009, pages 24-27. ISBN-13: 9789511236399

Lehto M. & Limnéll J. (2016). Cyber Security Capability and Case Finland, Proceedings of the 15th European Conference on Cyber Warfare and Security (ECCWS), 7.-8.7.2016 Munich, Germany, pages 182-190

Lehto M., LimnéllJ., Innola E., Pöyhönen J., Rusi T., Salminen M. (2017). Finland's cyber security: the present state, vision and the actions needed to achieve the vision, Publications of the Government´s analysis, assessment and research activities 30/2017. ISBN 978-952-287-368-2

Lehto M., Limnéll J., Kokkomäki T, Pöyhönen J, Salminen M. (2018). Strategic leadership of cyber security in Finland, Publications of the Government´s analysis, assessment and research activities 28/2018. ISBN 978-952-287-532-7

Ministry of Defence (2015). Finland, Guidelines for Developing Finnish Intelligence Legislation, Working group report, March 2015. https://www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf

Ministry of Transport and Communications (2016). Information Security Strategy for Finland The World's Most Trusted Digital Business Environment, Publications of the Ministry of Transport and Communications 9/2016. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78416/Publications_9-2016_Information_Security_Strategy_for_Finland.pdf?sequence=1

National Audit Office (2017). Performance audit report: Cyber Protection Arrangements, 16/2017. https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

Prime Minister's Office (2013). Central Government Communications in Incidents and Emergencies, Regulations, instructions and recommendations issued by the Prime Minister's Office 3/2013. https://vnk.fi/documents/10616/1093242/M0313_Central+Government+Communications+in+Incidents+and+Emergencies.pdf/e277d048-6ff2-481c-b678-41388e2b6cef/M0313_Central+Government+Communications+in+Incidents+and+Emergencies.pdf.pdf

Security committee (2013). Finland's Cyber Security Strategy and its background dossier, 24 January 2013 http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia

Security committee (2017a). Implementation Programme for Finland's Cyber Security Strategy 2017–2020. https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/126-suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020

Security committee (2017b). Security Strategy for Society, Government resolution, 2.11.2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Sylvain (Sly) Leblanc is an Associate Professor and Interim Chair for Cyber Security at the Royal Military College of Canada (RMC). Sly was a Canadian Army Signals Officer for over 20 years, where he developed his interest in computer network operations. His research interests are in computer security, cyber operations development and cyber education.

Wai Sze Leung is an associate professor at the Academy of Computer Science and Software Engineering at the University of Johannesburg. Her current research interests include digital forensics and the application of Artificial Intelligence in enhancing cyber security.

Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. His research interests include international security, intelligence reform, strategy, foreign policy analysis, European security policy and cyber security. Dr. Liaropoulos is also a member of the editorial board of the Journal of Information Warfare (JIW).

Jarno Limnéll is the Professor of cybersecurity in Aalto University, Finland. Martti Lehto is the Professor of cybersecurity in University of Jyväskylä, Finland.

Christoph Lipps graduated in Electrical and Computer Engineering at the University of Kaiserslautern. Born in Pirmasens, Germany in 1986, he started working as a Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs) and entity authentication.

Dr. Leandros A. Maglaras received the B.Sc. degree from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004, and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Volos, in 2008 and 2014 respectively. In 2018 he was awarded a PhD in Intrusion Detection in SCADA systems from University of Huddersfield. He is the head of the National Cyber Security Authority of Greece and a part time Senior-Lecturer in the School of Computer Science and Informatics at De Montfort University, U.K. He serves on the Editorial Board of several International peer-reviewed journals such as IEEE Access and Wiley Journal on Security & Communication Networks. He is an author of more than 100 papers in scientific magazines and conferences and is a senior member of IEEE.

Nnana Mogano is a professor of computing at University of Pretoria, South Africa. She received her Bachelor of Science in Statistics and Computer Science and Honours in Statistics from the University of Limpopo, South Africa in 2014. Her main interests are data analytics to enhance business models and operations.

Potsane Mohale is a master's student of the Academy of Computer Science and Software Engineering at the University of Johannesburg. He works as a software engineer based in Johannesburg, South Africa.

Pardis Moslemzadeh Tehrani is a Senior Lecturer in the Faculty of Law, University of Malaya where she has been a faculty member since 2015. Her research interests lie in the area of Cyber Terrosim, Human Right, International Humanitarian Law, Cloud Computing in Law. Pardis has widely published papers in a number of national and international Conferences.

Dr Jabu Mtsweni is a Research Group Leader for Cyber Defence at the Council for Scientific and Industrial Research (CSIR), Research Fellow at University of South Africa, and Advisory Board Member at ITWeb Security Summit. His research interests and technical expertise are in cyber warfare, cybersecurity, and cybercrimes. He has over 15 years academic and industry experience with over 60 peer-reviewed conference and journal articles.

Julie Murphy has over 10 years of experience in telecommunications working primarily with Fortune 500 companies, and currently works as a Security Expert with IBM X-Force Red. Julie lectures part-time in the Technological University Dublin and is actively involved in promoting cybersecurity awareness and training.

Abdalmuttaleb M.A. Musleh Al-Sartawi is the Editor-in-Chief of the International Journal of Electronic Banking (IJEBank). He received his PhD in Accounting, from UBFS. He has chaired as well as served as a member in various editorial boards and technical committees in international refereed journals and conferences.