Information & Security: An International Journal

Sarah Backman, vol.32, 2015 http://dx.doi.org/10.11610/isij.3206

ORGANISING NATIONAL CYBERSECURITY CENTRES

Sarah BACKMAN

Abstract: The emerging trend in practises of organising national cybersecurity management via national cybersecurity centres unifies preventive and reactive cybersecurity measures and moves towards an all-hazard approach. These centres constitute some of the most modern ways of organising national cybersecurity management and originate from a holistic view of cybersecurity. Based on the empirical examples from the UK, the US, Finland, Germany and The Netherlands, the paper identifies basic motivational aspects behind the creation of national cybersecurity centres, as well as common features, such as strategy documents, organisational frameworks, tasks and responsibilities. Moreover, this paper seeks to identify if the national cybersecurity centres appear to be successful. The paper finds that the national cybersecurity centres are given increasing amounts of resources, tasks, responsibilities and/or freedom of action by their governments. This implies that practices of organising national cybersecurity management in national cybersecurity centres has indeed been successful, and that the examined countries aim to further develop and empower them. The paper concludes in recommendations for organising national cybersecurity centres, drawing on the examples of the studied countries.

Keywords: National cybersecurity management, national cybersecurity centre, cybersecurity organisation, cybersecurity management practices, national cybersecurity strategy, digital development, United Kingdom, United States, Finland, Germany, The Netherlands.

Introduction

In recent years, several high-level policy documents have placed great emphasis on explaining the strategic importance of strengthening cybersecurity management and cooperation on this matter, both nationally and internationally. For example, the 2013 cybersecurity strategy of the EU underlined the need for both public authorities and private actors to develop their cybersecurity abilities and to cooperate in an efficient manner.[1]

Indeed, the presentation of the EU Cybersecurity Strategy in February 2013 was accompanied by a separate proposal for the so-called "NIS Directive," which stipulates a set of common standards and rules for ensuring a high level of Network and Information Security (NIS) across the Union.

Recognising that "there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness," the 2013 EU Cybersecurity Strategy called for EU legislation that would set out common minimum requirements for NIS at national level, obliging Member States to designate national competent authorities for NIS and to adopt a national NIS strategy and a national NIS cooperation plan.

This development derives from the fact that the digital development has caused extensive and intensive dependence on information and communication technology. Cybersecurity is now viewed as affecting and involving all parts of society, including economic, legal, technical, diplomatic and military aspects. At the same time, risks and threats linked to the digital environment are increasing.[2]

Since cybersecurity management is increasingly complex, involving society as a whole, it is widely acknowledged that enhancement of cybersecurity on the national level must be a shared responsibility, involving many kinds of actors and stakeholders. For instance, the 2010 Digital Agenda for Europe underlines the importance that both individuals, private and public bodies work together to improve cybersecurity – both in Europe as well as globally.[3] Also, the EU Cybersecurity Strategy states that all relevant actors need to take action in order to strengthen their resilience and achieve a coordinated response to the challenges of cybersecurity.

This view is not exclusive to Europe or the EU. For instance, the United States Five-Year Strategy (2014–2018) states that "Enabling the security of the Nation's critical cyber and communications infrastructure is a tremendously complicated undertaking requiring a concerted and sustained "whole-of-nation" effort to which individual citizens, private industry, government, and other partners all contribute."[4]

Recent national cyber strategies and policies seem to be reflecting this new, holistic view of cybersecurity management. For example, a comparative analysis of recent national cybersecurity strategies by the OECD shows that cybersecurity policy seems to become national policy priority, since cybersecurity is considered important for the security of the whole society. According to OECD, the new national cyber strategies also reveal that many countries have ambitions of enhancing governmental coordination regarding cybersecurity at both operational and policy-levels, and moreover making roles and responsibilities of the national cybersecurity management clearer.[5] Cybersecurity policy making seems to have developed and grown into a new, enhanced capacity, with better coordination and inclusion of different stakeholders.[6]

In recent years some countries have chosen to organise their national cybersecurity management practises in national cybersecurity centres (NCSCs) grounded in the holistic view of cybersecurity. These organisations are characterised by the unification of preventive and reactive cybersecurity measures. This paper aims to examine the emerging trend of organising national cybersecurity management in NCSCs. Based on the empirical examples from the UK, the US, Finland, Germany and The Netherlands, the paper seeks to identify motivational aspects behind the creation of NCSCs, but also their features such as strategy documents, organisational frameworks as well as common tasks and responsibilities. Moreover, this paper seeks to identify if this way of organising national cybersecurity management practises appears to be successful. The material used for preparing this paper includes mainly policy and strategy documents regarding cybersecurity, both from the EU and from the countries studied, as well as international reports on the subject.

Terminology issues of cybersecurity

Even if the awareness of the importance of handling cybersecurity at the national level is rising, both national and international cybersecurity policymaking entails complex challenges. Terminology is one of them. Terminology within the field of cybersecurity differs widely among nations, organisations and academia. This is partly due to the rapid development of the digital environment and a lack of standardisation for terminology in the area. Consequently, this could cause misinterpretations and become an obstacle in the communication among sectors, countries or actors. Statistical measurements in the area of cyber also become difficult, especially on the international level, since there can be a variety of names for the same sort of phenomena.[7]

For example, there are several alternative labels to what is commonly called Computer Security Incident Response Team, or CSIRT, an organisation performing cybersecurity incident handling and response.[8] For example:

- Computer Emergency Response Team (CERT);
- Computer Incident Response Team (CIRT);
- Computer Incident Response Centre (or Capability) (CIRC);
- Computer Security Incident Response Centre (or Capability) (CSIRC);
- Security Operations Centre (SOC);
- Cybersecurity Operations Centre (CSOC).

Labelling, but also tasks, responsibilities and size of CSIRTs vary. Even if they have the same core services, and often follow existing models of structure and activities, every CSIRT has its own characteristics.[9]

Since this paper aims to study national cybersecurity organisations, terminology naturally becomes a challenge and an issue that must be addressed. For example, the organisations examined in this paper did not all go by the label "National Cybersecurity Centre," even though they all have basically the same set of capabilities, tasks and responsibilities combining proactive (preventive) and reactive (management) measures at the national level. Some countries, such as the United Kingdom, use the term CERT to describe this organisation. Others, such as Finland and The Netherlands, actually use the term National Cybersecurity Centre.

In this paper, the term "National Cybersecurity Centres" (NCSCs) is used to describe organisations that:

- are the entities of their respective countries' national cybersecurity management;
- move towards an "all-hazard approach," referring to the fact that an organisation aims to prepare for all types of threats and to improve resilience;
- have both preventive and reactive capabilities;
- have responsibilities for international cooperation and participation in cybersecurity initiatives;
- have information-sharing capabilities;
- have coordinating tasks for the measures of national cybersecurity management.

Motivations behind the creation of National Cybersecurity Centres

Drawing on policy documents connected to the national cybersecurity centres of the UK, the US, Finland, Germany, and The Netherlands, a number of common motivational aspects behind the creation of the centres could be identified:

- Increased vulnerability;
- Need for expertise;
- Need for a comprehensive approach towards cybersecurity;
- The benefits of strengthening national cybersecurity management.

Increased vulnerability

The studied countries state that they are becoming increasingly dependent on the Internet. They find that all parts of society now use the digital domain and see an increasing connectivity, both between states, private parties, military and civilians, nationally and internationally. The Internet connects people worldwide and is considered by the countries to be of a huge advantage in many ways. However, the countries also recognise that dependence on it as well as the connectivity it creates leads to

greater vulnerability. Moreover, they know that new vulnerabilities are constantly emerging from all directions and in many different forms, due to the complexity of the cyber domain. New vulnerabilities can, for example, be a result of regular IT maintenance, a bad patch or an update.[10] This development has happened quite quickly, and the countries studied state that many organisations are still not even close to becoming resilient, and struggle with, for example, legacy systems and replacement of outdated systems that are still vital for them.

New light has been shed on this issue by the increasing number of cyberattacks lately, some of them resulting in incidents, which has been noticed by the countries studied. One of the best known incidents is STUXNET, a complicated malware program designed to disrupt industrial processes. STUXNET was discovered by experts in 2010.[11] A more recent attack was discovered in July 2012, when 10,000 email addresses of top Indian Government officials, including intelligence agencies, were hacked. Another example is the attack on the Estonian government networks in May 2007, resulting in disruption of government online services as well as online banking. Even though the Estonians responded well, the attack served as a wake-up call for many cyber-dependent countries, including those studied in this paper.[12]

The need for expertise

The countries studied recognise that cybersecurity management, especially at the national level, is highly complex and therefore requires considerable expertise, which the NCSCs can offer.

The need for expertise in order to manage national cybersecurity is also highlighted in the recently released report from ENISA (European Network and Information Security Agency), called Report on Cyber Crisis Cooperation and Management – Comparative study on the cyber crisis management and the general crisis management, which states that cyber crisis/incident management contains several additional challenges compared to generic crisis management. For instance, cyber incident management requires people with the necessary competence in order to understand the technical aspects of the incident to communicate these with decision-makers. Technical expertise is thereby a more important factor when handling a cyber-related incident compared to handling a generic crisis, when it comes both to analysis and response.[13]

Furthermore, the report suggests that a single organisation for national cybersecurity management, such as a NCSC, can contribute to bridging the gap between the technical and societal parts of national cybersecurity management and their different perspectives on cyber-related issues. For example, it is naturally harder for both public sector and decision-makers to understand the information from the technical cybersecurity functions, which results in difficulties in acting on it. Since the challenge is not only about differences in language, and in account of the fact that very few people

have both the technical and policy expertise, an extra knowledge broker such as a national cybersecurity centre is considered to be useful.[14]

The need for a comprehensive approach towards cybersecurity

The countries studied find that not only is the amount of digital data increasing, but that the current connectivity is more extensive than ever. They also recognise that both states and private parties act in the digital domain, and the interdependence of the civilian and military domains increases as well.[15]

Cybersecurity is therefore identified by the countries studied as a key aspect of protecting information structures on which the nations are highly dependent, and so cybersecurity is highlighted by the countries as critical for the resilience of the critical infrastructures, economy and national security, and demands cohesion in policy initiatives, public information and operational cooperation of multiple actors and parties.

The countries studied state in their national cybersecurity strategies that cybersecurity will likely continue to grow in importance, and that managing it will require major efforts both nationally, involving players from the state, industry and society, as well as internationally, in cooperation with other countries and multinational organisations, which required a comprehensive approach. In order to be properly prepared for managing the digital development, they identify that all parts of society, both individually as well as collectively, need to be transparent and to be able to cooperate and coordinate in an efficient manner. One problematic aspect of information-sharing between public and private actors is that it requires a high level of trust, and hence privacy and compliance are considered as increasingly important issues.

The countries studied strive for a comprehensive approach not least because the challenges of cyberspace tend to transcend national and sectoral borders. A reliable and secure information and communications infrastructure is important to provide international support in order to promote and strengthen international trade and security. Sustained partnerships are seen as a part of enhancing this. Formal and informal CSIRT networks are generally considered to be important sources for international information and support exchange.

The benefits of strengthening national cybersecurity management

The countries studied have identified a link between strengthening national cybersecurity and economic, social, political and security benefits. Cybersecurity serves to protect interests of individuals – such as privacy and the secure use of online services, but also organisational interests – such as availability and integrity, business and economic interests – such as safe trade environments, and consequently the interests of society as a whole.[16]

Drawing on this background, the countries in this study aim to strengthen national cybersecurity and consider the creation of national cybersecurity centres as a way of effectively achieving this. The national cybersecurity centres contribute to the effectiveness of national cybersecurity practise in multiple ways, including implementation of synchronised and therefore effectively performed cybersecurity measures, the maximum use of resources and minimum loss of information. They furthermore contribute to the quality of the cyber security situational awareness in an increasingly complex context, which is of great importance for decision-makers. An overview of the common motivational aspects behind the creation of such centres is depicted in Figure 1.

Common features of National Cybersecurity Centres

When studying the UK, the US, Finland, Germany, and the Netherlands, a set of common features of national cybersecurity centres could be distinguished regarding:

- National cybersecurity strategies;
- Organisational frameworks;
- Common tasks and responsibilities.

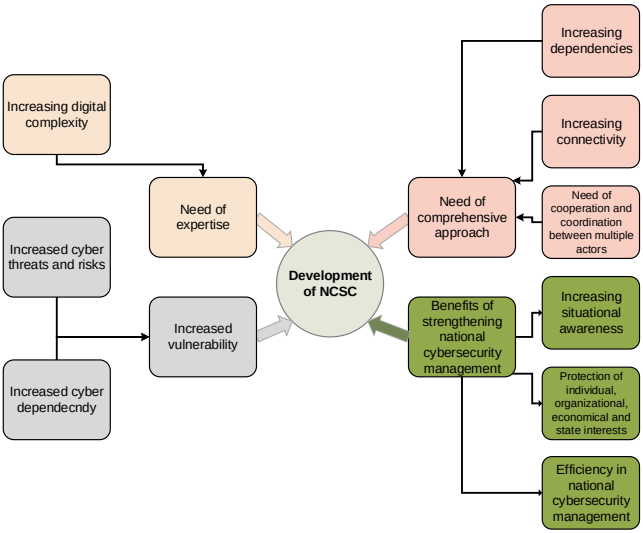

Figure 1: Overview of the common motivational aspects behind the creation of NCSCs.

National cybersecurity strategies

The countries studied prove that a national cybersecurity strategy can serve both as a way of explaining the analysis and identified needs behind the formation of the centres, the basic guidelines and frameworks for their establishment as well as the tasks, objectives and further development of the centre.

For example, the Dutch National Cybersecurity Centre was formed and came into operation in 2012 in order to meet the objectives set up in the first Dutch National Cybersecurity Strategy from 2011.[17] The second Dutch national cyber strategy[18] from 2014 in turn serves as an explanation of the Dutch Government's shift of focus from awareness-raising to capability-building measures as well as the further strengthening of the already established NCSC.

The creation of the Cybersecurity Centre of Finland in 2014, under the Finnish Communications Regulatory Authority (FICORA), was also based on government-identified requirements regarding national information security arrangements, formulated in the Finnish National Cybersecurity Strategy of 2013.[19] The Cybersecurity Centre would, thus, ensure needs such as efficient and wide-ranging information collection, an analysis and information gathering system, shared situational awareness, as well as national and international cooperation regarding preparedness.

Another example is the CERT-UK, the UK National Computer Emergency Response Team, which was formed in March 2014 in response to the 2011 UK National Cybersecurity Strategy.[20]

Likewise, the establishment of the German Cyber Response Centre, as well as the German National Cybersecurity Council (NCSC) was envisaged by the German Cybersecurity Strategy of 2011.[21] The German IT Situation Centre and the Crisis Reaction Centre were established in fulfilment of measures listed in the "National Plan for Information Infrastructure Protection" (NPSI) from 2005.

Organisational frameworks

The countries examined in this study show two basic types of arranging national cybersecurity management. One way is to have a national cybersecurity centre as one single unit with a set of national cybersecurity management tasks, CERT functions included. Finland and the Netherlands are examples of countries following this organising principle. The United Kingdom has organised the centre in a similar way, with its CERT-UK having four main responsibilities, from cybersecurity incident management to the promotion of cybersecurity situational awareness and international coordination as well as collaboration with other national CERTs.

Another way of organising national cybersecurity centres is to have several smaller units, each specialising on different cybersecurity tasks, and all performing under one large umbrella-unit for national cybersecurity management.

The US NCCIC, for example, has four different branches, which support each other and together form the capabilities, partnerships and authorities needed in order to lead the implementation of a national cybersecurity approach at the operational level. The NCCIC aims to uphold resilience in the cyber infrastructure by coordinating the prevention and mitigation of cyber risks and threats, enhance information sharing and improve the abilities of risk and incident management among partners, as the national centre of cyber and communications integration.

Another example of organising in this fashion is the BSI (Federal Office for Information Security) – the national cybersecurity authority of Germany. The BSI has organised the national cybersecurity measures in five information security departments, one central and four specialised. The departments handle, for example, cybersecurity, security consulting and coordination, cryptographic technology as well as standardisation and certification. Each department consists of one or two divisions, each of which in turn comprises a number of sections. The purpose of the BSI is to promote cybersecurity in Germany by providing central IT security service to the federal government but also to private actors.

Both NCCIC and BSI have CERT as one of the specialised units underneath the national cybersecurity umbrella-unit. In addition, both of them have internal coordination functions. For example, the NCCIC's branch Operations and Integration (NO&I) synchronises analysis, information sharing and incident response efforts across the NCCIC branches and activities.

Common tasks and responsibilities

- *Creating cybersecurity pictures and situational awareness*

In order for the NCSC to perform its tasks and responsibilities, it must understand the context and environment in which it operates – at all levels. This is referred to as *situational awareness*.[22]

Tasks and responsibilities for all of the studied centres involve creating national situational awareness through a single comprehensive picture of the cybersecurity situation. Since cybersecurity issues are both technically and generically complex, having a joint picture of the situation is considered to be highly valuable for strategic decision-making. In order to create a single comprehensive picture of the cybersecurity situation, the centres usually gather information which could come from, for example, trend reports, cooperation networks, national as well as international partners, but also from monitoring input.

In Finland, for example, the input to the cyber security situational awareness comes from information about cyber abnormalities and threats (nationally and internationally) which is combined with results from inspections of information systems and data communication. This becomes evaluated and analysed, and then distributed among the stakeholders. The stakeholders then estimate the effects of it on their activities, and share this analysis with the centre again. The centre finally puts this information into the national cybersecurity situational awareness.

One of the essential issues when it comes to maintaining cybersecurity situational awareness that improves stakeholders' understanding of trends, threats and developments in the digital domain, is information sharing.

- *Enhancing and coordinating private-public partnerships and information sharing*

The countries studied state that effective cybersecurity management at the national level at current requires both extensive, intensive, national and international information sharing and coordination. Sharing of information between stakeholders in networks, not least about incidents, improves learning as well as understanding of the current cyber threat situation. An active and coordinated network will also increase the level of knowledge of the members in the cooperation networks.

In enhancing and creating structures and networks for information sharing among stakeholders—public, private, national and international—the NCSCs evidently play major roles, not least regarding the development of much needed methods that allow information sharing between private entities and other actors without risking sensitive information being leaked.

The NCSCs' tasks often include normative guidance and responsibility for the development of generic templates and models for cooperation and collaboration. The countries examined have identified collaborative measures and unified responses to the challenges of cybersecurity as key aspects of enhancing national cybersecurity management. Since one weak link could affect everyone, as many stakeholders as possible must be included in the efforts.

Collaboration and cooperation among, for example, local actors, private actors and state governments are considered to be increasingly important in order to enhance national cybersecurity. This was, for example, the background to the creation of the Dutch National Cybersecurity Strategy (NCSS1) launched in 2011, called "Strength through cooperation." Another example is the German National Cybersecurity Strategy of 2011, which stated that "the public and the private sector must create an enhanced strategic and organisational basis for closer coordination based on intensified information sharing."

In the US, enhanced collaboration and cooperation is considered to be a highly important measure. The NCCIC branch ICS-CERT's main focus is on public-private partnerships, and it is tasked, besides from providing situational awareness of critical infrastructure and key resources stakeholders, to work towards strengthening cybersecurity partnerships.

- *Advising and offering expertise*

One of the common main responsibilities of the NCSCs is providing both public and private actors with advisory and expert services on cybersecurity issues, for example, giving recommendations when vulnerabilities are detected. The Netherlands even offer advice-support to other countries in order to strengthen their CERTs, since they consider it to be beneficial that other countries increase their ability to handle cyber risks and threats.

- *Incident management and support*

In addition to advisory services, a common function of the cybersecurity centres is support and coordination of response by private, public, or decision making actors regarding disruptions, incidents or crises. This is considered to be valuable since swift countermeasures are highly important when handling cyber incidents or crises, as these can develop quickly and lead to large-scale damage in short periods of time. For example, the US-CERT works as an incident response centre, which means that it is 24/7 standby to accept, triage and collaboratively respond to incidents and give technical advice to information system operators. The US-CERT is independent of the other worldwide CERT organizations, but may coordinate with them on security incidents.

- *Enhancing and participating in international cooperation initiatives regarding cybersecurity*

Strengthening international cooperation in the field of cybersecurity is a common objective of the NCSCs, and the importance of cooperation between national CERTs is emphasised. In order to meet the objectives of further enhancing international cooperation, involvement of the NCSCs in international cybersecurity initiatives and existing structures of cooperation as well as active participation in national and international exercise activity in order to uphold the expertise of the personnel are some of the measures prioritised. Flexibility and mutual trust are seen as being essential for these collaborations to work, but active participation in the cybersecurity activities of international organisations could provide important opportunities to exchange information, lessons learned and best practices with international actors and improve the national quality of cybersecurity. Common actions on cybersecurity challenges are considered to be highly important.

Networks of experts and practitioners on cybersecurity, for instance among different CERTs, are regarded as important in order to exchange information and increase knowledge of cyber issues.

This view is reflected in a number of high-level policy statements and commitments at national as well as international level. Increased information sharing and the use of channels and mechanisms for information sharing are considered also as a confidence-building measure, which could improve timely response, recovery and mitigation activities.

Figure 2 below presents the identified common tasks and responsibilities of the national cybersecurity centres, subdivided into preventive or/and reactive capabilities.

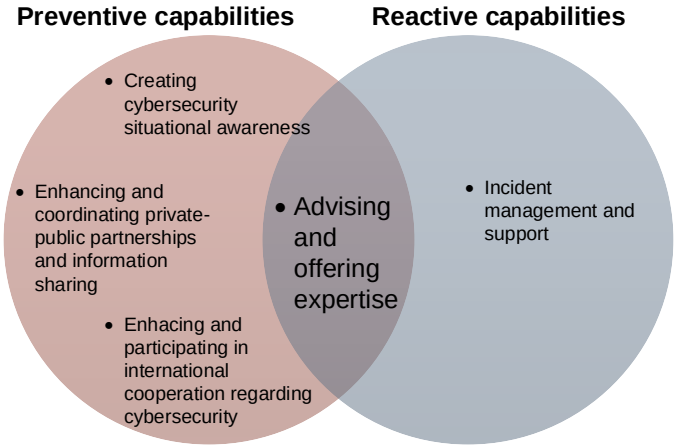

Figure 2. Identified common tasks and responsibilities of the NCSCs.

The trend of further developing National Cybersecurity Centres

A trend in the further development of established national cybersecurity centres can be identified by studying policy documents and statements regarding the NCSCs of the UK, the US, Finland, Germany and The Netherlands.

All of the countries of this study have continuously strengthened their national cybersecurity centres, and plan to do so onwards. This development is highlighted by the increasing amount of resources, tasks, responsibilities and/or freedom of action they are given by their governments. For example, since its launch, The Netherlands' Cybersecurity Centre has turned into a spider in the web of the public-private cybersecurity networks, and is now tasked to develop further due to its detection

capability and its role in a crisis. In accordance with the German Digital Agenda 2014–2017,[23] the German BSI will also be continuously strengthened and given additional resources in its cybersecurity management tasks and objectives, while the German National Cyber Response Centre will be given an enhanced role regarding coordination and management of cybersecurity incidents.[24] In the case of Finland, the vision of its NCSC is that it will develop further into a national and international cyber authority which will be able to provide greater variation of information security services.[25] In the UK, CERT-UK has continuously been given new tasks. For example, it is now tasked to deepen its bilateral and multilateral networks, and lead a new programme of joint exercising with the US. It became also responsible for running the digital environment of "Cyber Security Information Sharing Partnership" (CISP) [26] — a collaborative initiative of information sharing regarding cyber threats and vulnerabilities between industry and government. As an example of increasing freedom of action, the US recently approved "The Federal Cyber Security Act of 2015,"[27] which stated that cybersecurity is now a top national priority, allowing acceleration of the use of the cyber intrusion detection and prevention system run by the department of Homeland Security, which analyses federal agencies network traffic in order to identify and stop cyber threats.

Recommendations

Based on the examples of the studied countries, national cybersecurity organisations that:

- are the entities of their respective countries national cybersecurity management;
- are moving towards an "all-hazard approach," i.e. the organisational model aims to provide for meeting all types of threats and to improve resilience;
- have both preventive and reactive capabilities;
- have responsibilities of international cooperation and participation in cybersecurity initiatives;
- have information sharing capabilities;
- have coordinating tasks in the implementation of measures of national cybersecurity management

... could be used to deal with, for instance:

- the vulnerability created by the increased cyber-dependency for all parts of society combined with increased cyber threats and risks;
- the need of expertise created by increased cyber complexity;

- the need of a comprehensive approach due to connectivity, dependence and the need for cooperation and coordination between multiple stakeholders and actors

... are commonly preceded by a national cybersecurity strategy that:

- outlines visions and objectives of the national efforts towards enhanced cybersecurity;
- explains the analysed and identified needs behind the formation of the centre;
- serves to provide basic guidelines and framework for the establishment as well as for stipulating the main tasks and further development of the organisation

... aim to provide the following advantages:

- protection of interests for the whole of society, including individual, business, organisational, economic and state;
- increased efficiency of national cybersecurity measures, maximum use of resources and minimum loss of information;
- increased situational awareness;
- support for decision-makers

..and have main tasks and responsibilities such as:

- creating national cybersecurity pictures and enhancing situational awareness;
- enhancing and coordinating private-public partnerships and information sharing;
- advising and offering expertise on cybersecurity issues;
- offering incident management and support;
- enhancing and participating in international cooperation initiatives in the field of cybersecurity.

Conclusion

This paper examined practises and emerging trends in organising national cybersecurity management, with focus of national cyber security centres (NCSCs) which unify preventive and reactive cybersecurity measures and reflect a holistic view of cybersecurity.

When examining the countries of this study, the motivations behind the development of NCSCs appear to be grounded in similar general conclusions about the challenges that come with the use of cyberspace today, such as:

- increased vulnerability – deriving from increased cyber threats and risks, and increasing cyber dependency;
- the need of expertise – deriving from the increasing digital complexity;
- the need of a comprehensive approach – due to increasing connectivity, dependencies, and the need of cooperation and coordination between multiple actors.

Organisational approaches reflect also opportunities created by strong and efficient cybersecurity management, such as the protection of individual, organisational, economic and state interests, and increased efficiency in national cybersecurity management. This does not appear to differ among the countries studied.

Establishing a NCSC is ultimately a way for the countries studied to effectively respond to the identified cybersecurity challenges, as well as utilising the opportunities of cyberspace.

Despite differences in size and in the ways of splitting responsibilities, the NCSCs examined in this study show some common features:

- national cybersecurity strategies outline visions and objectives of the national efforts towards enhanced cybersecurity, explain the analysed and identified needs behind the formation of the centres, and serve to provide basic guidelines and frameworks for the establishment as well as for the main tasks and further development of the organisations;
- organisational frameworks provide either for arranging the national centre as one single unit with a set of national cybersecurity management tasks, or to have several smaller units, each specialising on different cybersecurity tasks under one large umbrella-unit of national cybersecurity management;
- common tasks and responsibilities such as creating situational awareness, enhancing and coordinating private-public partnerships and information sharing, advising and offering expertise, providing incident management and support, and enhancing as well as participating in international cooperation initiatives regarding cyber security. This may be a result of the similar conclusions about the general challenges that come with the use of cyberspace today, and of the similar perceptions about suitable measures for dealing with these challenges. This finding is promising, since it could facilitate international cybersecurity standardisation, management and cooperation.

Moreover, this paper also attempted to identify if organising national cybersecurity management practices in NCSCs appears to be successful. The author found that the studied centres are given increasing amounts of resources, tasks, responsibilities and/or freedom of action by their governments, and that the examined countries aim to further develop and empower them. This implies that organising national cybersecurity management in this way has indeed been successful, and also indicates that the identified common strategy documents, organisational frameworks, tasks and responsibilities of the centres have been suitable and doable.

Drawing on the success of the already established NCSCs, and the fact that the awareness of the importance of handling cybersecurity at the national level is rising internationally, there is a reason to believe that the emerging trend of organising national cybersecurity management via NCSCs will continue, and that more countries will follow the examples of the UK, the US, Finland, Germany and The Netherlands.

Acknowledgement

The author would like to extend her gratitude to Roger Holfeldt, CEO of Secana, for providing insight and expertise, and for supporting the research of this paper. The author would also like to thank Baris Uckan, risk management specialist at Secana, for comments that improved the manuscript.

Notes:

[1] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," 2013, available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[2] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace."

[3] European Commission, "A Digital Agenda for Europe," 2010, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0245&from=EN.

[4] US Department of Homeland Security, Fiscal Years 2014–2018 Strategic Plan, 2014, available at: http://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

[5] OECD, "Cybersecurity Policy Making at a Turning Point – Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy," 2012, available at: www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282011%2912/final&doclanguage=en.

[6] OECD, "Cybersecurity Policy Making at a Turning Point."

[7] ENISA, "Report on Cyber Crisis Cooperation and Management – Comparative Study on the Cyber Crisis Management and the General Crisis Management," 2014, available at

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study.

[8] Carson Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," MITRE, 2014, available at https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

[9] Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center."

[10] ENISA, "Report on Cyber Crisis Cooperation and Management – Comparative Study on the Cyber Crisis Management and the General Crisis Management."

[11] CSIS, "Significant Cyber Incidents since 2006," accessed on 05 June 2015, available at: http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf.

[12] CSIS, "Significant Cyber Incidents since 2006."

[13] ENISA, "Report on Cyber Crisis Cooperation and Management."

[14] ENISA, "Report on Cyber Crisis Cooperation and Management."

[15] OECD, "Cybersecurity Policy Making at a Turning Point."

[16] OECD, "Cybersecurity Policy Making at a Turning Point."

[17] The Netherlands National Cybersecurity Strategy, 2011, available at www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

[18] The Netherlands National Cybersecurity Strategy 2, 2014, available at www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf.

[19] Finland's Cybersecurity Strategy Government Resolution, 2013, available at http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

[20] Cabinet Office, UK Cyber Security Strategy, November 2011, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[21] Federal Ministry of the Interior, Cybersecurity Strategy for Germany, February 2011, available at www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

[22] Carson Zimmerman, MITRE, "Ten Strategies of a World-Class Cybersecurity Operations Center"; Office of the President of the US, International Strategy for Cyberspace, 2011, available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf.

[23] The Federal Government, Germany: Digital Agenda 2014 – 2017, 2014, available at http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6.

[24] Federal Office for Information Security, The State of IT Security in Germany 2014, 2014, available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile.

[25] Kommunikationsverket, Cybersäkerhetscentrets Verksamhetsplan 2014–2016, 2014, available in Finnish at www.viestintavirasto.fi/attachments/Cybersakerhetscentret_Verksamhetsplan_20142382112016.pdf.

[26] Gov.UK, Policy Paper "2010 to 2015 Government Policy: Cyber Security," available at www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

[27] S.1869, The Federal Cybersecurity Enhancement Act of 2015, available at www.ronjohnson.senate.gov/public/_cache/files/a06a1865-e219-43e6-aaee-7017f39f60b2/fcea-one-page.pdf.

SARAH BACKMAN is a consultant at Secana focusing on matters of cybersecurity and crisis management. Secana is a risk management company that offers expertise and objective strategic advisory in risk and crisis management for societal security with emphasis on cyber security. The company is a part of Ekelöw Group led by Ekelöw InfoSecurity AB. Secana helps customers on the national and international levels to find solutions to complex security challenges and problems based on their local requirements and environment. The company is currently the leading Swedish provider of cybersecurity services for both the private and public sectors.
Sarah's primary tasks at Secana involve different types of analysis, research and evaluation, and she is a key contributor to Secana's involvement in academia and research in general. Sarah has published a number of reports, articles and papers. Sarah Backman has a background from the Swedish Defence University where she studied political science focusing on crisis management, international cooperation, security policy and strategy. Moreover, she has studied theory about organisations, security policy and crisis management in European practice, as well as European law. Currently, Sarah Backman is pursuing a Masters in Politics and War at the Swedish Defence University. *E-mail*: Sarah.Backman@secana.se