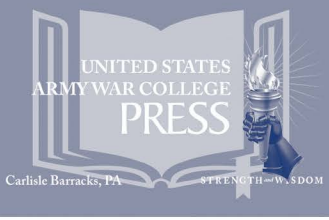
The Letort Papers



CYBER DEFENSE: AN INTERNATIONAL VIEW

Keir Giles
Kim Hartmann

Strategic Studies Institute
U.S. Army War College, Carlisle, PA

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Defense: An International View	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Strategic Studies Institute,47 Ashburn Drive,Carlisle,PA,17013-5010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**64**	

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership and Development contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

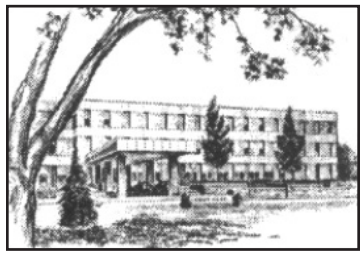
The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The Senior Leader Development and Resiliency program supports the United States Army War College's lines of effort to educate strategic leaders and provide well-being education and support by developing self-awareness through leader feedback and leader resiliency.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

CYBER DEFENSE: AN INTERNATIONAL VIEW

Keir Giles
Kim Hartmann

September 2015

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudies Institute.army.mil*, at the Opportunities tab.

*****

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

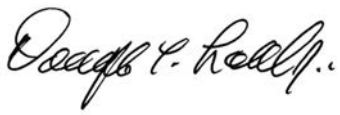
ISBN 1-58487-697-2

FOREWORD

Because of the seamlessly international nature of the Internet, effective cyber security demands close cooperation with allies and friends overseas. Yet, because of the relatively young status of the discipline, national approaches to organizing and providing for cyber defense vary widely even among those countries whose interests are most closely aligned with those of the United States. The result is that the bodies and structures responsible for cyber defense, and their affiliations and mandates, can be difficult to understand.

In this Letort Paper, British cyber policy researcher Keir Giles and German computer security specialist Kim Hartmann provide an overview of four different national approaches to cyber defense: those of Norway, Estonia, Germany, and Sweden. While providing a useful guide for engagement with the relevant governmental and other organizations in each of these countries, the Paper also compares and contrasts the advantages and drawbacks of each national approach.

In doing so, the authors provide a valuable resource for policymakers in the cyber security field, identifying potential best practices that could be applied in the United States and elsewhere.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHORS

KEIR GILES is the director of the Conflict Studies Research Centre (CSRC), a group of deep subject matter experts on Eurasian security formerly attached to the United Kingdom (UK) Ministry of Defence. Now operating in the private sector, CSRC provides in-depth analysis on a wide range of security issues affecting Russia and its relations with overseas partners. After beginning his career working with paramilitary aviation in Russia and Ukraine immediately following the fall of the Soviet Union, Mr. Giles joined the BBC Monitoring Service (BBCM) to report on political and military affairs in the former Soviet space. While attached from BBCM to CSRC at the UK Defence Academy, he wrote and briefed for UK and North Atlantic Treaty Organization (NATO) government agencies on a wide range of Russian defense and security issues. Uniquely, he is a double Associate Fellow of the Royal Institute of International Affairs (Chatham House) in London, UK, as well as a regular contributor to research projects on Russian security issues in both the UK and Europe. Mr. Giles's work has appeared in a wide range of academic and military publications across Europe and in the United States.

KIM HARTMANN has been employed at the Institute of Electronics, Signal Processing and Communication at Otto von Guericke University, Magdeburg, Germany, since 2011, where she conducts applied research in secure network design principles, risk analysis and assessment of networks, network components, and protocols. Ms. Hartmann is a regular contributor to research projects and conferences on cyber and network security, including the annual North Atlantic Treaty

Organization Cooperative Cyber Defense Center of Excellence CyCon event. Her academic work specialized in computer security and mathematical modelling, protocol security analysis, computer security risk assessment, and risk analysis of critical network infrastructures. Ms. Hartmann studied Computer Science and Mathematics at the Royal Institute of Technology, Stockholm, Sweden; and Otto von Guericke University, Magdeburg, Germany.

SUMMARY

Despite the history of offensive cyber activity being much longer than is commonly thought, cyber defense is still considered a new discipline. It is only relatively recently that states have established formal structures to provide for cyber defense, and cyber security more broadly. In this context, each nation has developed its own mix of public, private, and military organizations active in the field.

The relationships between these organizations are based on the nation's unique circumstances, determining the overall shape of relations between the state and business, the approach to e-government, civilian control of the military, threat perception, and much more. The United States is no exception and has developed its own approach to organizing cyber defense based on factors specific to it. But the wide range of organizational approaches to reaching a "best fit" template for successful cyber defense raises the possibility that other nations may have developed approaches that could be usefully adopted in a U.S. context.

This Paper introduces four different foreign approaches to cyber defense, each very different from the U.S. model. In surveying the cyber defense organizations of Germany, Sweden, Norway, and Estonia, the Paper aims not only to provide baseline information on overseas structures and planning in order to facilitate U.S. cooperation with international partners, but also to provide policymakers with an overview of effective alternative approaches that may be applicable in a U.S. context.

CYBER DEFENSE: AN INTERNATIONAL VIEW

Despite the history of offensive cyber activity being much longer than is commonly thought, cyber defense is still considered a new discipline.[1] It is only relatively recently that states have established formal structures to ensure cyber defense, and cyber security more broadly. In many nations, these structures are still in a state of flux as the optimum approach to defense against cyber threats for the military, the economy, the government, and the population as a whole is still elaborated.

In this context, each nation has developed its own mix of public; private; and military organizations, and the relationships between them based on their own unique circumstances—relations between the state and business, approach to e-government, civilian control of the military, threat perception, and much more. The United States is no exception and has developed its own approach to organizing cyber defense based on factors specific to the United States.

But the broad variety of organizational approaches to reaching a "best fit" template for successful cyber defense raises the possibility that partner and ally nations may have developed approaches that can be successfully adopted in a U.S. context. This Paper therefore surveys the approaches of four partner states, in order to present them in an easily accessible form for U.S. policymakers. In introducing foreign approaches to cyber defense that may not be obvious in a U.S. context, the aim is also to provide baseline information on overseas structures and planning to facilitate U.S. cooperation with international partners.

The Paper is specifically not concerned with technical capabilities in cyber offense and cyber defense. It is notoriously difficult to reach reliable conclusions about cyber capabilities from open sources. The extent of real capabilities, or in some instances the lack of them, is so deeply classified that an unclassified publication on the subject would consist mostly of unfounded speculation. Nevertheless, in some European societies with a tradition of openness of information, it is possible to draw inferences about organizational aspects of preparations for cyber defense, as opposed to actual capabilities, on the basis of open sources and direct approaches to defense organizations.

The countries selected for examination are Estonia, Germany, Norway, and Sweden, in that order. This is because:

1. **Estonia** has a number of claims to pioneer status in cyber defense. This state has practical experience of protecting itself against offensive online activity combined with a real-world destabilization campaign, in what is widely (if questionably) considered the first overt state-on-state cyber attack in May 2007. Tallinn is host to the North Atlantic Treaty Organization (NATO) Combined Cyber Defence Centre of Excellence (CCDCOE), set up in 2008 in what was widely (but again, wrongly) considered to be a response to those attacks. Estonia is at the forefront of moving government services online; personal identification acts as a key to an impressive range of services that other states consider unsafe to operate through the Internet. Governmental and societal embrace of the Internet is exemplified in the President of the Republic, Toomas Hendrik Ilves, an enthusiastic participant in social media, Internet freedom activist, and chair of the "Panel on the Future of Global Internet Coop-

eration," a body set up by the Internet Corporation for Assigned Names and Numbers to develop future principles for Internet governance. For all of these reasons, Estonia presents a useful case study of what can be achieved if the political will to implement radical change is present.

2. **Germany** represents a major economy, guided by (broadly) the same principles as the United States with regard to the balance between security and individual rights and freedoms online but subject to historical, institutional, and European constraints that do not apply to the United States. In this respect, Germany offers an example of a G7 state (United States, Japan, Germany, France, United Kingdom, Italy, and Canada) that has chosen a different model to protect its online networks.

3. **Norway** is in a unique position within Europe, being an active and enthusiastic member of NATO, but remaining outside the European Union (EU). The constraints and opportunities for Norway's foreign and defense policy therefore differ from those of other states, and this singularity is reflected in a number of specific Norwegian approaches to security and economic challenges. Close cooperation with the United States is one of these opportunities.

4. **Sweden** has, in some ways, the reverse challenge. As a member of the EU but not of NATO, Sweden (along with its neighbor, Finland) has to maintain a delicate balancing act. The benefits of close cooperation with the United States and NATO are clear and unarguable, but this is a topic of intense domestic sensitivity. Sweden's traditionally robust and independent stance on defense issues has come under threat,[2] but the emphasis on cyber security—and on the international cooperation necessary to maintain

it—remains strong. In addition, Sweden presents the paradox of a society that traditionally has been among the most open and democratic in the world, hosting defense and intelligence programs, including in the cyber sector whose secrecy is more closely guarded than those of almost all European partners.

For each of these countries, a survey of institutions and declaratory policy on the basis of publicly available documentation has been supplemented by interviews with officials active in cyber security. In each case, while these officials were willing to confirm details of national cyber security structures, they did not wish to be identified or linked to specific comments. The summaries at the end of each national section and in the conclusion are in part based on these non-attributable interviews.

It will be seen that there are both synergies and dissonances between the national approaches adopted by each of these states. These national approaches remain crucial in the apparent absence of real supranational support for cyber defense. Even after the Wales Summit in September 2014, NATO's cyber strategy appears to remain an anti-strategy, devolving cyber defense to member states.[3] Meanwhile, the EU's European Network and Information Security Agency (ENISA) appears similarly to limit its ambition to being a center for expertise and information sharing.[4]

ESTONIA

Estonia is reputed to be the country with the world's highest Internet penetration rate. In December 2011, this rate was already 78 percent.[5] This results from deliberate government policy rooted in the early days of Estonia's renewed independence in the early-1990s. At that time, Estonia took the strategic decision not to attempt to renew or overhaul the wholly insufficient and backward Soviet telecommunications system, and instead adopted modern systems such as mobile phone networks in parallel. The result is a highly advanced technical infrastructure, with few of the problems of reliance on legacy telecommunications systems and hardware that have restrained Internet uptake elsewhere.

A further strategic decision was to develop systems to provide state services to all citizens online, in part as a result of Estonia's relatively low population density. The development of these e-services made Estonia a world leader in the field and contributed to Estonia's impressive record of post-Soviet growth. However, as the 2007 attacks on Estonia showed, it also presents vulnerabilities. Estonia therefore presents an example of an approach to protecting cyber infrastructure and critical data where not only is a key adversary already known and present, but also the concentration of citizen processes online (including but not limited to banking, voting, registering commercial transactions, and so on) means that there is no alternative to reliable defense.

General Structure.

Cyber security in Estonia is mainly organized through the Estonian Information System Authority (EISA) and its subunits. EISA is part of the Ministry of Economic Affairs and Communications but may also cooperate closely with the Ministry of Justice, Ministry of Defense, and Ministry of the Interior.

In addition, the Defense League (Kaitseliit), a voluntary defense organization along military lines, also contributes to "the protection of Estonia's independence and constitutional order." A cyber unit cooperates closely with governmental institutions and initiatives. Known as the Küberkaitseliit, this is made up of volunteer cyber security experts.

Detail.

EISA.

EISA, also known by its Estonian abbreviation RIA, was reorganized in 2011 from the former Estonian Informatics Centre and is structurally integrated in the Ministry of Economic Affairs and Communications.[6] EISA coordinates cyber security actions for both the private and public sector. These activities include the development, administration, and supervision of cyber security actions.[7]

EISA publishes an annual report summarizing events, activities, and observations related to cyber security in Estonia.[8] EISA is also taking part in the *NutiKaitse 2017* project promoting security on smart devices and aimed at users, developers, and retailers.[9]

EISA is the governing authority of two other bodies, Department of Critical Information Infrastructure

Protection (CIIP) and Computer Emergency Response Team of Estonia (CERT-EE), which are discussed next. EISA also provides the Document Exchange Centre and supervises the implementation of *Infosüsteemide Kolmeastmeline Etalonturbe Süsteem* (three-level information technology [IT] baseline security system), abbreviated ISKE, at the national level. ISKE is based on the German *IT-Grundschutzkatalog* (see the section on Germany for further details).[10]

EISA also provides information on the Data Exchange Layer X-Road. X-Road is described as being "a technical and organizational environment, which enables secure Internet-based data exchange between the state's information systems."[11] Furthermore, EISA is involved in the management, maintenance, and support of the national Public Key Infrastructure (PKI). This implies involvement in supporting the Estonian identification (ID) card system, used to provide secure access to many online services.[12]

Department of Critical Information Infrastructure Protection.

CIIP is a subunit of EISA. CIIP focuses on "issues associated with the protection of technical infrastructures needed to guarantee the functioning of the Estonian state." The Estonian Emergency Act provides a list of 42 essential services that need to be assured, including payments and settlements.[13]

CIIP operates on the strategic level by collecting, maintaining, and analyzing data regarding critical information infrastructures in Estonia. CIIP also performs risk assessment for these infrastructures, and initiates and supervises the development and implementation of protective measures.[14]

Linked to its actions on the strategic level, CIIP issues guidelines on cyber security, such as the regulation on security measures for information systems of vital services and related information assets[15] and the Estonian *Cybersecurity Strategy 2008-2013*.[16]

CIIP operates under the information security interoperability framework,[17] a description of IT-security principles observed in Estonia and how state institutions and vital service providers are to interoperate.[18]

CIIP recommends security measures based on a number of foreign best practice manuals. These are the U.S. Cyber Consequences Unit Cyber-Security Check List, in a version last updated in 2007;[19] ISKE, based on German documentation as described previously; and the United Kingdom (UK) Centre for the Protection of National Infrastructure (CPNI) Guidelines on Supervisory Control and Data Acquisition (SCADA) Security.[20]

ISKE provides a range of documentation on security guidelines that, unlike much other materials, are only available in Estonian.[21] These include:

- ISKE material and handbook (*ISKE juhendid ja materjalid*)
  - Implementation guidelines (*ISKE rakendusjuhend* ver. 7.00)[22]
  - ISKE catalogue version 7.0 (*ISKE kataloogid* ver. 7.00)[23]
- Suggested guidelines (*Soovituslikud juhendid*)
  - Data center security requirements (*Andmekeskuse turvanõuded*)[24]
  - Cryptographic algorithms, uses, and life cycle study (*Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring*).[25]

Computer Emergency Response Team of Estonia.

The CERT-EE is another subunit of EISA. CERT-EE defines its main tasks as:

- Reviewing and reporting on incidents;
- Providing warnings and notices, and the organization of preventive measures such as campaigns to raise public awareness; and,
- Support for institutions and Internet Service Providers (ISPs). The extent of support depends on the security incident reported and the resources available. As a general policy, no end-user support is given.[26]

As a subunit of EISA, CERT-EE also provides and develops the Virtual Situation Room (VSR) in cooperation with Clarified Networks Finland,[27] acquired by the Finnish-U.S. corporation Codenomicon in 2011.[28] VSR, financed by the European Regional Development Fund, is a unified platform used for cyber security situation information sharing, analysis and visualization of data, providing training material and simulations, and post-crisis analysis and crisis management improvement techniques.[29] VSR is accessible to governmental institutions and companies providing vital services.[30]

Küberkaitseliit.

Küberkaitseliit is the cyber unit of the Defense League (Kaitseliit). The Kaitseliit is "a voluntary militarily organized national defense organization" that possesses arms, engages in military exercises, and fulfils the tasks prescribed by the National Defense League Act.[31] Its cyber subdivision is made up

of cyber security professionals who volunteer their time and skills for national defense, with main tasks listed as:

- Protection of Estonia's e-lifestyle,
- Public-private cooperation in protecting IT infrastructure, and
- Knowledge and information sharing.

The Küberkaitseliit supports government institutions in implementing the national cyber security strategy and—especially in a crisis situation—cooperates closely with CERT-EE and the Ministry of Internal Affairs.[32]

Summary.

The Estonian approach to cyber security rests on a clear division but smooth cooperation between state actors, the public sector, and the Estonian Defence League. This is supported by extensive public documentation and a clear sense of purpose from government.

Estonia also makes strong contributions to European and international cooperation on cyber security, but not all public documentation is provided in languages other than Estonian. This is surprising in the case, for instance, of the ISKE, which is based on the German BSI-Grundschutzkatalog, a document that is already—at least partially—available in English.

The establishment of overarching structures to facilitate cooperation between providers of essential services is a priority. Estonia actively promotes the individual's role in cyber security issues, the need for infrastructures that allow smooth interaction, high-quality communications, and the integration of

nonstate institutions and companies in national cyber strategies.

Estonia has embraced the concept that cyber conflict cannot be resisted through governmental institutions alone, but must rather be approached through the collaboration of government institutions, nongovernmental organizations, and private sector companies.

GERMANY

The first German strategies on a federal level to protect technical infrastructure against malfunction arose in response to the "millennium bug." As elsewhere, during the 1990s, automation of technical communication, transportation, information, and organization systems had risen in importance for military, governmental, and industrial organizations in Germany. The Y2K problem raised national awareness of vulnerabilities accompanying reliance on technical systems. The potential effect on individual citizens primarily was gauged as a factor of their dependence on national or industrial services; home computers, laptops, and other technical equipment used for private purposes were not considered targets of national relevance.

The importance of protecting technical infrastructure against both deliberate and accidental destruction, disturbance, and malfunction was publicly acknowledged during the first years of the 21st century. The establishment of the first federal strategic program to protect technical infrastructures in 2002 was immediately tested by a natural disaster—unprecedented flooding that severely affected a number of European countries.[33] Widespread malfunctions of technical infrastructure throughout the affected area

hindered emergency management and increased the damage. The result was greater acknowledgement of the need to protect technical infrastructure and greater prominence of the effects on individual citizens in public discussion. Nevertheless, awareness of risk associated with privately used information technology is still deficient, both within civil society as well as in industrial, government, and occasionally even military applications.

General Structure.

The Cabinet of Germany (*Bundesregierung*) is the chief national executive body at federal level. It consists of the elected chancellor (*Bundeskanzler*) and the cabinet ministers.[34] Each cabinet minister is responsible for one specific sector of national interest. The responsibility for these sectors is currently divided among 14 federal ministries.[35] Overlaps between the scope of these ministries can occur, and this is particularly the case when considering protection against cyber threats.

Figure 1 lists some of the many ministries and their associated special agencies that are involved in cyber defense in Germany. Interactions between the following institutions in particular are key to understanding the German approach to cyber security and will be discussed further:

- The German Chancellery
  - Federal Intelligence Service (*Bundesnachrichtendienst*)
- Federal Ministry of the Interior
  - Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik, BSI*)

  - Federal Agency for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*)
  - Federal Criminal Police Office (*Bundeskriminalamt*)
- Federal Ministry of Defense
  - Military Counterintelligence Service (*Militärischer Abschirmdienst*)
  - Federal Defense Forces of Germany (Bundeswehr)
    - Strategy Reconnaissance Command (*Kommando Strategische Aufklärung, especially the Abteilung Informations und Computernetzwerkoperationen*)[36]
- Federal Ministry of Finance
  - Customs Criminal Investigation Office (*Zollkriminalamt*)
- Federal Ministry of Economics and Technology

Detail.

Due to the complex federalized nature of German administration, many German cyber defense activities are managed through joint programs. This is in part a result of legal constraints arising from constitutional emphasis on division between state, civilian, and military actions, which means that activities within each sector must be clearly distinguishable from those in another. As a result, synergies between each responsible agency are limited. For example, even if a joint program allows military institutions to cooperate with the police, this can only happen if the specific incident under investigation is a clearly defined military responsibility.[37]

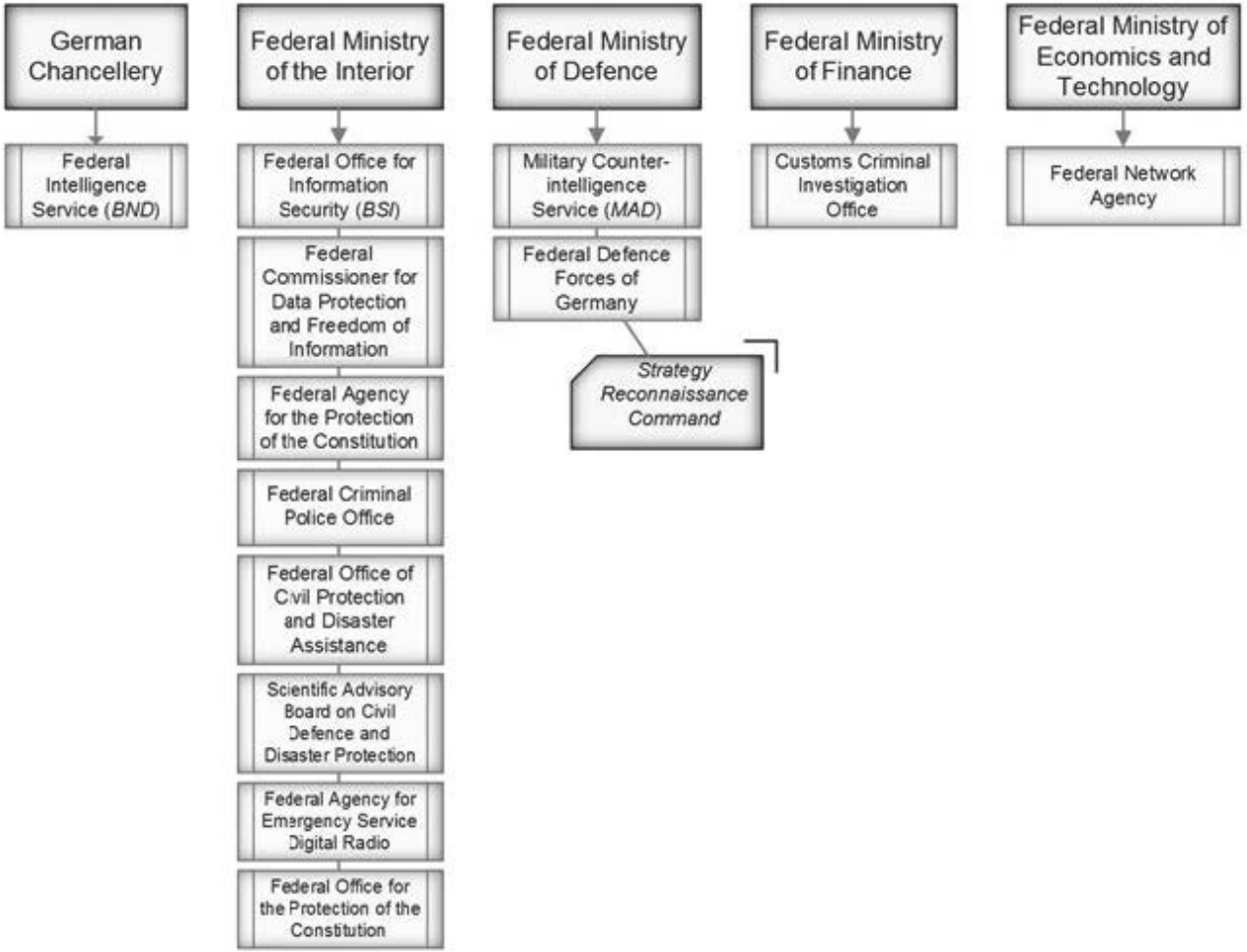


Figure 1. Selection of German Ministries and Departments Involved in Cyber Defense.

KRITIS.

Several programs have been developed to meet a range of challenges associated with the protection of critical infrastructures, referred to generically as KRITIS. The primary programs are UP KRITIS (*Umsetzungsplan* KRITIS),[38] UP Bund (*Umsetzungsplan Bund*)[39] and KRITIS-*Strategie*.[40]

The two UP programs were developed in 2005 from the previous "*Nationaler Plan zum Schutz der Informationsinfrastrukturen*" (National Plan for Information Infrastructure Defense, NPSI) program.[41] While UP KRITIS is concerned with the general protection of IT infrastructure of the telecommunication, energy, transportation, and economic sectors, UP Bund covers the protection of federal IT infrastructure. Both UP programs are considered policymaking institutions; technical implementation of recommendations made through the UPs becomes the responsibility of sectors and organizations for which they are responsible.

KRITIS-*Strategie*, the "National Strategy for Critical Infrastructure Protection," was drawn up in 2009 on the basis of knowledge gained from UP KRITIS, and summarizes Germany's objectives and strategic political approach in this area. The Strategy extended the initial remit of the program and included IT infrastructure as one of the critical infrastructures to be protected.[42] Protection of IT infrastructure has been allocated to the National Cyber Defense Center and the National Cyber Security Council, created under the *Cybersecurity Strategy* released in 2009.[43]

The National Cyber Defense Center.

The National Cyber Defense Center was established as a response to growing threats, in particular the increasing number of highly specific and organized attacks on governmental and industrial information systems in Germany. The Center coordinates the numerous ministries, departments, and special agencies involved in national cyber defense. In this way, the existence of the Center underlines the German view that cyber attacks come in a variety of forms and vectors, and as such must not be addressed through only one federal institution.[44]

The Center is operated by the Federal Office for Information Security (BSI) and includes representation from the Federal Agency for the Protection of the Constitution, Federal Office of Civil Protection and Disaster Assistance, Federal Criminal Police Office, Federal Police, Customs Criminal Investigation Office, Federal Intelligence Service, and the Federal Defense Forces of Germany (*Bundeswehr*). Each agency contributes personnel with specific responsibilities, who remain affiliated to their original office. As a result, implementation of tasks assigned within the Center become the responsibility of the contributing agency. The Cyber Center also cooperates directly with German ISPs.

The Center's main tasks are the prevention of cyber attacks, information sharing on attacks and vulnerabilities, and early warning for exposed and threatened institutions. According to the BSI, the Center analyzes and reports on vulnerabilities found in IT products, incidents, infrastructural vulnerabilities, and cyber attack methods. It also analyzes incidents to generate attack and attacker profiles. The Center is the technical

adviser to the National Cyber Security Council (*Cyber Sicherheitsrat*), which was founded simultaneously with the Center.

Due to the scope of the institutions involved, and control resting with the BSI, the Center is more likely to be a reactive than a proactive or offensive institution and is mainly concerned with incident response, forensics, and policy actions. The German military organization corresponding to the Cyber Center is the *Kommando Strategische Aufklärung*. Oblique references in open sources suggest that the *Kommando* has been developing offensive cyber capabilities[45] since, at the latest, 2009.[46]

*The National Cyber Security Council***.**

The main task of the Council is to enhance exchanges between governmental and industrial organizations on preventive cyber measures on a political and strategic level. Recent topics for discussion have been the protection of critical infrastructure and the cyber foreign policy of Germany.

The Council meets three times a year and is chaired by the Commissioner of the Federal Government for Information Technology. The Council is composed of one state secretary and representatives from the German Chancellery, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defense, the Federal Ministry of Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Research, and representatives of the federal states Baden-Württemberg and Hessen. Furthermore, business representatives from the BDI (Federation of German Industries), BITKOM (Federal Association for Information Tech-

nology, Telecommunications and New Media), DIHK (Chambers of Commerce and Industry), and Amprion (the largest corporation responsible for the German electricity distribution network, with a major role in European electricity distribution more broadly[47]) act as associated members of the Council. Technical experts may also be involved in specific events.[48]

IT Baseline Protection Catalogs.

The IT Baseline Protection Catalogs (*IT-Grundschutzkataloge*) are a collection of documents provided by the BSI for the protection of IT infrastructure and the identification and eradication of vulnerabilities in IT systems. They serve as a basis for certifying enterprises for IT security compliance. They are divided into three sub-catalogs covering components, threats, and measures. Each uses a layer model to describe different aspects of the topic presented.

The component catalogs are divided into five layers: general aspects, infrastructure, IT systems, networks, and IT applications. Each layer is addressed to a specific audience.[49] They describe different methods and actions to be taken for each IT component in different situations. Recommendations are provided throughout the component life cycle.[50]

The threat catalogs describe the range of vulnerabilities associated with IT components and are divided into the following layers: *force majeure,* organizational deficiencies, human failures, technical failures, and deliberate acts.[51] Each threat and its source is briefly described, followed by examples of possible outcomes and their effects on the component.

The measures catalogs describe the countermeasures to be taken in order to protect systems, subdivided into Infrastructure, Organizational, Personal, Hardware/Software, Communication, and Emergency Response.[52] Each countermeasure identifies the individual responsible for initiation and execution, followed by a specific description of the actions to be taken. The measures catalogs also provide checklists to monitor correct implementation and to verify the results.

As noted in the section on Estonia, which has based some of its own documentation on these catalogs, a number of these documents are also available in English.[53]

CERTs.

As in other states, the term Computer Emergency Response Team (CERT) refers to a group of IT experts consulted during serious incidents. CERTs exist within a range of organizations and businesses. The key governmental CERTs are the *Bürger*-CERT (Public CERT), CERT-*Bund* (CERT-Federal), and the CERTBw (CERT Federal Defense).

The *Bürger*-CERT provides technical information on IT vulnerabilities, viruses, worms, cyber attacks, and methods through information boards, newsletters, and mailing lists to technically interested individuals. This is a free service provided through the BSI, using data obtained from the CERT-*Bund*.[54] A second service, aimed to inform the broader public (i.e., including individuals who are not technically adept), is provided through the BSI on the website BSI *für Bürger* (BSI for Citizens).[55]

The CERT-*Bund* and the *IT-Lagezentrum*[56] together make up Department C-21 of the BSI.[57] Within the department, the CERT is the technical solution center for security issues faced in federal institutions, while the *IT-Lagezentrum* collects security data from multiple national and international sources. Together, this allows Department C-21 to provide detailed assessments of security issues. Depending on the result of this assessment, warnings may be forwarded to the *Bürger*-CERT or the relevant KRITIS authorities.[58] It is reported that the *IT-Lagezentrum* not only relies on the data pools provided, but also carries out network monitoring "to detect irregularities."

The CERTBw is the Federal Defense Forces (*Bundeswehr*) CERT. The CERTBw is responsible for the monitoring, maintenance, and restoration of IT security for the German military forces. Its responsibilities also include incident response and management and network monitoring and analysis. CERTBw also analyzes vulnerabilities in the German military IT infrastructure, analyzes malware, and provides an information and alert service.

CERTBw reports that the number of hostile incidents it deals with has remained steady at 700-800 per year for the last 4 years.[59] This figure is startlingly low. When asked to explain this, one interviewee suggested that this could be a result of the strict delineation of authorities within the German system, which would mean that attacks on public-facing military websites would not be included in this figure:

> Perhaps one should rather say [the CERTBw reporting] 'counts approx. 800 incidents per year on technical infrastructures lying within its area of responsibility'? I also think that the number is incredibly low and, knowing the German system, I believe the reason is

> that a lot of stuff will not fall under their authority. I could imagine that for example the public sites of the German Forces are not part of the CERTBw authority and so on.[60]

The CERTBw is also responsible for the security of IT infrastructure used during active military operations.[61]

Summary.

Overall, Germany seems to promote an open access policy regarding its cyber defense strategies. Both policy documents and technical details are available from official websites. Once the infrastructure and organizational details are clear, further details can be deduced from official job offers, which often include specifics of the level of knowledge needed, the type of technical infrastructure to be worked on, and the tasks to be undertaken during employment.[62] Even organizational details not directly available through agency websites normally can be accessed through the *Bundesverwaltungsamt* (Federal Office of Administration).[63]

NORWAY

General Structure.

Public attention to the defense of cyberspace has increased enormously in Norway over recent years.[64] *Cyberforsvaret* (Cyber Defense) is a *forsvarsgren* (military branch) of the Norwegian Armed Forces alongside the Norwegian Air Force, Army, Navy, and Home Guard. The *Cyberforsvaret* was established in 2012,

denoting Norway as one of the countries that officially acknowledge cyberspace as a new military domain. The integration of cyberspace as a military branch expresses the importance of the topic to the Norwegian government.

Other institutions involved in the cyber defense programs of Norway under the auspices of the Armed Forces include *Nasjonala Sikkerhetsmyndigheten* (National Security Authority, or NSM)[65] and the Norwegian Computer Emergency Response Team (NorCERT). Furthermore, depending on the type of attack experienced, either the *Etterretningstjenesten* (Norwegian Intelligence Service, the intelligence service of the Norwegian Armed Forces) or the Norwegian Police Service may respond to an attack with further investigations.

The police service is responsible for any attack/criminal activity on the Internet originating from within Norway against Norwegian infrastructures or individuals; it investigates the attack and initiates further activities. The *Politiets sikkerhetstjeneste* (Norwegian Police Security Service**)** and *Kripos* (*nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet*, former *Kriminalpolitisentralen*, translated to National Criminal Investigation Service) are involved in the investigations as appropriate. In addition, the Norwegian government has established the *Norsk senter for informasjonssikring* (Norwegian Center for Information Security, NorSIS), to heighten public awareness of cyber threats and possible countermeasures.

Detail.

*Cyberforsvaret***.**

Established on September 18, 2012, as an independent military branch of the Norwegian Armed Forces, *Cyberforsvaret* evolved from the *Forsvarest informasjonsinfrastruktur* (Defense Information Infrastructure) department of the Norwegian Armed Forces and has a manpower of approximately 1,100.[66] The main task of *Cyberforsvaret* is to establish cyberspace (cyberrommet) as a full-fledged military domain.[67] It is responsible for the development of defense methods for cyberspace and for the protection of military components from threats originating from cyberspace. *Cyberforsvaret* is not responsible for protection of public infrastructure but may support public organizations such as NorSIS upon request.

Cyberforsvaret is organized into two major departments, responsible for "competence and transformation" and "services and operations" with several subdepartments. The branch is scheduled to introduce offensive cyber capabilities by 2016,[68] noting that:

> Military operations in the digital space have both protective and intelligence purposes and offensive objectives/goals. This has been an added dimension of military operations and thus a new warfare area where the ability to conduct both defensive and offensive operations will be crucial in future conflicts.[69]

Cyberforsvaret is currently offering research positions in cyber security. Researchers are to be integrated and employed in the newly established Center for Cyber and Information Security (CCIS) at the Gjøvik University College. The CCIS is the result of a part-

nership between "key national cyber security stakeholders."[70] The CCIS thus provides significant detail on the nature and extent of cooperation on cyber security between Norwegian military, police, and public institutions.[71]

Nasjonala Sikkerhetsmyndigheten.

The NSM is a sub-division of the *Försvarsdepartmentet* (Defense Department) and is responsible for the coordination of preventive security measures and for monitoring the current security status. The NSM's primary tasks are countermeasures against espionage, sabotage, and terrorism, and the protection of sensitive information.

The NSM is Norway's key body responsible for the control and organization of information and physical security activities. Although the NSM belongs to the *Försvarsdepartmentet,* it also reports to the *Justis- og Politidepartment* (Ministry of Justice and Public Security) with respect to public information security interests.[72] The NSM also publishes annual reports on Norway's security status (*Rapport om sikkerhetstilstanden*)[73] and is the host organization for NorCERT.

NorCERT.

NorCERT is the operational taskforce of the NSM. NorCERT reports on current cyber security threats that may pose a risk to national security and may also take part in incident response and analysis. Although NorCERT is hosted by the NSM, it also cooperates closely with a range of nongovernmental bodies in the *varslingssystem for digital infrastruktur* (warning system

for digital infrastructures, or VDI). The VDI was initiated as a joint project between the *Etterretningstjenesten*, *Politiets sikkerhetstjeneste* (Intelligence Service, Police Service) and NSM in 2000.[74]

The VDI controls a number of sensors installed at ISPs to monitor data traffic. VDI sensors had been installed at *Norsk rikskringkasting AS,* NRK (Norwegian Broadcasting Corporation—a government owned radio and television broadcasting company)[75] in 2006, but NRK decided to remove them amid widespread controversy over data capture and monitoring in November 2012.[76]

NorSIS.

NorSIS forms part of a Norwegian government initiative to heighten public awareness of cyber security threats and their impact on everyday life as well as on national security and is hosted by the *Justis- og beredskapsdepartmentet* (Ministry of Justice). Its major task is to inform, analyze, and recommend countermeasures against cyber security threats for the public. NorSIS is responsible for both the private and public sector, and may request support from *Cyberforsvaret* or NorCERT. NorSIS also compiles guidelines and recommendations for improving IT security overall.[77]

Summary.

Norway is responding to a significant number of attacks against its infrastructure.[78] Despite numerous activities to heighten cyber security, there is still concern about Norway's vulnerability as a nation dependent on its IT systems.[79] Despite the fact that Norway has only recently begun to integrate cyber defense on

a national level, previous achievements leave Norway well placed to be one of the best equipped European countries for cyber defense. The VDI sensors, in place since 2000, provide network-specific security and surveillance, while, to some extent, disregarding privacy issues.

In 2012, Vidar Sandlad, senior consultant to NorSIS, observed that one key cyber security problem is the naivety of the Norwegian public.[80] Programs and education provided by NorSIS and the information campaigns established by the Norwegian government are heightening awareness and knowledge of computer security. Norway appears to be experiencing less difficulty in communicating to its public the vital role of individuals in ensuring cyber security than does Sweden.

SWEDEN

General Structure.

The cyber defense strategies of Sweden are organized primarily through two ministries and their subdepartments: the Ministry of Defense and the Ministry of Justice. The Ministry of Defense is in charge of eleven divisions, both military and civilian:[81]

- Swedish Armed Forces (*Försvarsmakten*)
- Swedish National Defense Radio Establishment (*Försvarets radioanstalt*)
- Swedish Defense Research Agency (*Totalförsvarets forskningsinstitut*)
- Swedish Defense Materiel Administration (*Försvarets materielverk*)
- Swedish National Service Administration (*Rekryteringsverket*/former *Pliktverket*)

- Swedish National Defense Export Agency (*Försvarsexportmyndigheten*)
- *Försvarsunderrättelsedomstolen* (a court responsible for the judicial review of defense operations)
- Swedish Coast Guard (*Kustbevakningen*)
- Swedish Civil Contingencies Agency *(Myndigheten för samhällsskydd och beredskap)*
- Swedish Defense Intelligence *(Statens inspektion för försvarsunderrättelseverksamheten)*
- Swedish Accident Investigation Board (*Statens haverikommission*)

The divisions known to be involved in the cyber defense of Sweden are the Swedish Armed Forces, the Swedish National Defense Radio Establishment (FRA), and the Swedish Defense Research Agency (FOI).

Under the Ministry of Justice, a sub-department of the Swedish Police (*Svenska Polisen*), the *Säkerhetspolis* (Swedish Security Service, or SÄPO) is also involved in cyber defense activities. SÄPO is generally concerned with national security issues, such as counterterrorism, counterespionage, protection of the constitution, and protection of officials. However, according to official documents, the SÄPO is also responsible for the replacement and maintenance of security related IT components of the Swedish police. A specific example given is "signal protection material" (*Signalskyddmatriel*), referring to any component used to protect communications.

The sub-departments of the Ministry of Defense may be considered responsible for threats originating from outside Sweden, including military actions, while the SÄPO and its associated divisions exist to

protect Sweden against terrorism, espionage, and violations of the constitution. Interaction between the Department of Defense sub-departments and the SÄPO is much stronger than in other countries in Europe, which demand a strict delineation between military and civilian operations.

Detail.

*FRA***.**

Although it is subordinate to the Ministry of Defense, the FRA is a civilian institution. It is responsible for the surveillance of civilian and military communication, as well as the establishment, maintenance, and support of IT security in governmental institutions and public enterprises.

The FRA is mostly known for its comprehensive monitoring of data communications. Monitoring methods and the Titan communications storage database are controversial issues within Sweden. The existence of Titan was disclosed in a Swedish television report on FRA collection and storage methods in June 2008.[82] It is not disclosed to what extent the FRA stores communication content and metadata.

The FRA may monitor communications on orders from the Swedish government, the Chancellery, the Ministry of Defense, the Swedish Criminal Investigation Department (*Rikskriminalpolisen*), or the SÄPO. These orders must be approved by the *Försvarsunderrättelsedomstolen*, a court responsible for the judicial review of defense operations.

As a result of adjustments to numerous laws collectively referred to as *FRA-Lagen*, the FRA officially is now allowed to monitor Swedish communication

links constantly. The data collected is stored up to 12 months and may legally be exchanged with other nations and research institutions.

Communications monitoring assets available to the FRA include the HSwMS Orion (A201) SIGINT vessel and two Gulfstream IV aircraft. In 2010, it was announced that the outdated Orion would be replaced by a new warship by 2015. The Swedish government announcement included a statement that ". . . currently the Baltic Sea is safe."[83] Although the new vessel is mentioned repeatedly in the context of observations of the closer seas, this could also imply that the Orion is to be substituted by a ship more suitable for overseas operations as well.

The annual FRA budget was intended to be increased by almost 5 percent to SEK (Swedish krona) 860 million (approximately $118 million) in 2014.[84]

Military Intelligence and Security Service.

The *Militära underrättelse- och säkerhetstjänsten* (Military Intelligence and Security Service, MUST) is a division of the Swedish Armed Forces and cooperates closely with the FRA, FOI, and others. However, MUST is also known to work with the SÄPO on a regular basis to expand intelligence and security services to civilian areas.

MUST is an intensely security-conscious organization, to the extent that (according to interviewees) staff names are not available even in internal documentation and directories, which refer only to number sequences or aliases. This operational security measure is intended to counter foreign recruiting, blackmail, and observation actions targeting MUST employees due to their knowledge of current operations and

capabilities. Interviewees note the effect that this has on former colleagues with a public profile disappearing entirely from view when joining a Swedish intelligence agency, a process some refer to as "going into the fog." They also highlight the exotic nature of a process such as this in a country like Sweden, which is sufficiently open and public that the Royal Family's tax declarations are available online.

With reference to IT security, MUST's annual report states that it has been involved in the acquisition, setup, integration, and verification of technical components. It also notes that, since 2013, it has acknowledged that technical components may be manipulated and impose an IT security risk. MUST referred particularly to doctored computer mice sending data to external observers, manipulated components including backdoors for attackers, and incidents that seem to refer to unrecognized transmission of data through USB.[85]

As a result of concerns like these, MUST verifies any technical equipment prior to its installation within the Swedish Armed Forces or its other clients. In 2013, MUST also published an internal document describing methods to establish and maintain the security and confidentiality of material in various areas, including IT systems. Despite the document not being intended for external distribution, a version was accessible through the *Försvarsmaktens* file server.[86]

*IT-Försvarsverbandet***.**

The *IT-Försvarsverbandet* (ITF) is a division of the Swedish Armed Forces, known to cooperate with MUST. The ITF focuses on IT threats, whereas MUST operates as both an intelligence and security agency with IT being just one of the areas covered.

Little information has been released on the ITF, but a combination of newspaper reporting and the organization's public job advertisements show that the ITF employs an unknown number of IT forensic specialists as well as operating system developers.[87] It recruits individuals capable of analyzing network traffic and code, capable of exploiting zero-day actions in systems, and having a profound knowledge of the execution of cyber attacks. It cooperated with the respected KTH forensic laboratory in analysis of the Flame virus detected in Stockholm in December 2012, which led to speculation on personnel transfer between the two organizations.

SÄPO.

SÄPO is the nonmilitary Swedish Intelligence Agency and is under the jurisdiction of the Swedish Police National Board. It is involved in protection of IT infrastructure, recruiting, and employing experts to install, maintain, and verify components. The SÄPO may also support MUST with investigations. Interviewees suggested that in contrast to Germany, Sweden historically has "not been strict" with separation of powers between military and civil security.

FOI.

The Defense Research Agency (FOI) engages in research rather than operations, but it benefits from direct access both to public and military policy researchers and to technical experts. As a result, it delivers some of the most significant reports on the IT security situation in Sweden. In particular, these include reports on:

- The risk of social media usage by employees within the Swedish Armed Forces.[88]
- The risk involved in the handling of tasks needing varying levels of security and confidentiality by one user on a single piece of equipment. Within this report, the need for development of a so-called reactive network was raised. This reactive network would be capable of automatically adjusting network security policies to the current actions performed by the user.[89]
- The risk associated with the widespread use and dependency of Swedish infrastructures on wireless communication. FOI discussed easily accessible jammers and their use by criminal organizations to disrupt Swedish investigation services, emergency response actions and police operations.[90]

Summary.

All states experience a wide disparity between the perception of cyber security risk by the government and by members of the public. In Sweden, this gulf seems particularly broad. Although the Swedish population is well-educated and accustomed to using IT from an early age, general disinterest in the risk of individual attacks poses a national threat. This disinterest may be a function of Swedish attitudes to and understanding of privacy.

Privacy and breaches of privacy are terms often dependent on the sociocultural background of the user. In some respects, Sweden is an exceptionally open-minded and public society. Furthermore, its citizens are generally prosperous, which means that the prospect of minor financial losses is not critical. These

two factors may lead to the public having a rather casual interest in the security of their electronic devices, which lowers the acceptability of security measures.

Sweden considers itself well-protected against attacks originating from outside the country, but Swedish networks are vulnerable to internal attacks. At the same time, the relaxed attitude to privacy works in Sweden's favor by providing a permissive environment for government monitoring of communications. In November 2013, Swedish Foreign Minister Carl Bildt defended surveillance practices, including cooperation with foreign intelligence partners, by saying, "We have one of the clearest, most law-abiding and probably best systems in this regard. I would think that other countries see us as a role model." Bildt successfully deflected criticism, defending the FRA law and arguing that there was sufficient transparency and oversight of its methods.[91]

Swedish decisionmakers recognize the risk posed by individuals to Swedish national cyber security, thanks to high connectivity and widespread use and dependency on IT. They are beginning to respond to this attitude by developing automated security tools that operate without the involvement of the user.

Despite Sweden being one of the most open societies in Europe, military activities in cyber defense are kept more confidential than in any other country surveyed. This is a reflection of a broader, and perhaps paradoxical, acceptance of the role of the military as a security provider and the necessary level of secrecy this entails. Interviewees felt that the large areas of Sweden designated for national security activities that are inaccessible to the public and only reached through nonsignposted private roads was sufficiently noteworthy to be brought to the interviewer's

attention; in many other countries, the existence of closed military areas would be entirely normal and uncontroversial.

This may be a legacy from the pervasive nature of Cold War preparations for total defense against Soviet aggression. One classic example is the plan for dispersed basing of the Swedish Air Force during hostilities, including the use of roads as runways, which has had an enduring effect on the layout of some sectors of Swedish highways. Interviewees suggested that as a result, major infrastructure projects in Sweden must receive approval from the defense forces due to the risk that changes to transportation, energy, or other networks may interfere with critical but undeclared capabilities. This extends to the cyber domain: adaptation of communications networks must receive approval due to the risk of disrupting sensitive surveillance, monitoring, or other capabilities.

The combination of several factors makes Sweden one of the better protected countries within Europe. These include:

- strong (cyber) border surveillance through the FRA;
- one central controlling unit protecting Swedish network infrastructure;
- the willingness of the Swedish public to accept and support data monitoring; and
- generous laws allowing cutting-edge government research on cyber attack methods and system exploits.

CONCLUSION AND IMPLICATIONS FOR U.S. POLICYMAKERS

Each nation reviewed in this Paper has developed a distinctive organizational structure it considers (at present) the best fit for providing for cyber defense, given its own unique societal, political, and constitutional circumstances. Fundamentally, however, the cyber challenges each of these states faces are very similar to those facing the United States. As a result, this review of national approaches to organizing cyber defense shows national initiatives that may be helpful when considered for development in the United States, but it also illustrates some models and constraints U.S. policymakers would specifically wish to avoid.

Estonia.

Estonia has the key advantage of being a small and cohesive society, unified by a generally shared threat perception and benefiting from advanced infrastructure and an impressively forward-thinking national government and president. This results in Estonia being a recognized role model within Europe and a vigorous promoter of international cooperation on cyber defense issues.

Estonia's wholesale adoption of e-services and e-government, while facilitating economies and growth, accepts risk of vulnerabilities. In mitigation, the country explicitly promotes civil integration in ensuring robust cyber defense. One interviewee noted that:

> Estonia has understood that cyber war cannot be responded to through government institutions alone, but must rather be approached through the collabora-

tion of governmental institutions, non-governmental organizations and private sector companies.[92]

For U.S. policymakers, Estonia provides a case study of risk versus benefit involved in the moving of government and commercial services online, as well as NATO becoming a proactive and forward-leaning partner in facilitating collective cyber defense.

Germany.

Germany seems to promote an open-access policy regarding its cyber defense strategies, including releasing a surprising depth of technical detail on security standards in both German and English. This policy must present a useful resource to any adversary seeking to circumvent and subvert those standards.

The dispersed nature of the cyber defense structure has a perceived advantage in that no central institution presents an attractive single target for attack, just as no single exploit can compromise infrastructure as a whole. But at the same time, despite the copious public documentation, Germany's federal system and constitutional constraints make it difficult to establish which agency is responsible for defending against which threat; this potentially presents an even greater challenge for foreign partners such as the United States, which seeks to increase cooperation with Germany.

Norway.

Norway's response to the challenge of cyber defense still appears to be in active development. But it has already achieved an impressively compact and simple organizational structure, in sharp contrast to Germany.

The sense of vulnerability resulting from dependencies on IT networks is well developed—a problem accented by the aim of finding economies of administration in areas with very low population densities. But Norway has been proactive in communicating the role of the individual in national cyber security (and overcoming "national naivety"), thereby limiting cyber defense vulnerabilities arising from internal networks. This has resulted in a public education effort with markedly greater impact than in Germany or Sweden.

Sweden.

Sweden, too, expresses official concern at the lax attitude of citizens to "cyber hygiene," and the resulting potential for increasing vulnerability to cyber attacks at the organizational or national level. This is in contrast to Sweden's reportedly robust defenses against attacks originating outside Sweden, thanks to a long-standing and proactive interest in close control and monitoring of international communications traffic passing into and through the country. In some respects, Sweden has filled the role of a regional cyber defense champion. Past cooperation between the FRA and U.S. and UK partner agencies has been highlighted in media reporting, and Sweden has acted as the *de facto* provider of some aspects of cyber defense

for Finland, pending legislative reforms intended to allow Finnish security agencies to inspect their own data traffic.[93]

Effective implementation of cyber defense principles is likely facilitated by the relative secrecy in which they are applied, as noted earlier. In the absence of the formal supranational relationship provided by shared membership of NATO, this makes it difficult to assess from open sources the extent to which effective cooperation between Sweden and the United States can be further developed.

In short, each national approach has its own advantages and deficiencies.

Advantages.

Germany provides clear national technical security advice; Estonia is strong in developing and installing technical solutions to ensure security; Norway has a robust public education program; and Sweden has invested heavily in protecting itself against external threats.

Deficiencies.

Germany suffers from a highly complicated federal system where responsibilities may overlap or leave gaps; Estonia accepts a degree of risk in its almost universal move of government services online; Norway is still expanding the capabilities of its recently established cyber defense forces; and Sweden experiences difficulty involving its public in cyber security measures.

Each of these provides a case study against which the United States can benchmark and validate its own cyber defense assumptions.

ENDNOTES

1. Jason Healey, "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012," Utica, NY: Cyber Conflict Studies Association, June 2013.

2. For more on this topic, see Stefan Forss and Colonel (Ret.) Pekka Holopainen, *Breaking the Nordic Defense Deadlock*, Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2015.

3. "NATO and Cyber Defence," NATO website, available from *www.nato.int/cps/en/natohq/topics_78170.htm*, accessed on September 20, 2014.

4. "What does ENISA Do?" Athens, Greece: European Network and Information Security Agency (ENISA) website, available from *www.enisa.europa.eu/about-enisa/activities*, accessed September 20, 2014.

5. Internet World Stats, Miniwatts Marketing Group, available from *www.internetworldstats.com/europa.htm#ee*, accessed on August 15, 2014.

6. Estonian Information System Authority, Tallinn, Estonia: January 3, 2014, available from *https://www.ria.ee/about-estonian-information-system-authority/*, accessed on January 9, 2014.

7. A detailed description of EISA's activities may be found at *Activities of RIA*, *ibid*., May 16, 2012, available from *https://www.ria.ee/activities-of-ria/*, accessed on June 2, 2014.

8. *2013 Annual Report Cyber Security Branch.* Estonian Information System Authority, Tallinn, Estonia: Estonian Information System Authority, July 7, 2014, available from *https://www.ria.ee/public/Kuberturvalisus/2013-annual-report-cyber-security-branch.pdf*, accessed on September 9, 2014.

9. *Look @ World Foundation,* Tallinn, Estonia: Vaata Maailma SA, available from *www.vaatamaailma.ee/en/nutikaitse*, accessed on September 9, 2014.

10. *Bundesamt für Sicherheit in der Informationstechnik* (German Federal Office for Security in Information Technology, hereafter BSI), *Grundschutzkatalog*, 2013, available from *https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf*, accessed on July 30, 2014.

11. *X-Road*, Tallinn, Estonia: Estonian Information System Authority, December 17, 2013, Data Exchange Layer X-Road, Estonian Information System Authority, available from *https://www.ria.ee/x-road/*, accessed on September 6, 2014.

12. Public Key Infrastructure PKI, Estonian Information System Authority, July 18, 2012, available from *https://www.ria.ee/public-key-infrastructure/*, accessed on September 2, 2014.

13. Emergency Act, passed June 15, 2009, available from *www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=en&sk=et&dok=XXXXX26.htm&query=H%E4daolukorra+seadus&tyyp=X&ptyyp=RT&fr=no&pg=1*, accessed on August 26, 2014; also available from *https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/520052014004/consolide*, accessed on September 2, 2014.

14. Critical Information Infrastructure Protection, Estonian Information System Authority, available from *https://www.ria.ee/ciip/*, accessed on December 2, 2014.

15. Regulation: Security Measures for Information Systems of Vital Services and Related Information Assets, Adopted March 14, 2013, Information System Authority, available from *https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf*, accessed on September 2, 2014.

16. *Küberjulgeoleku strateegia 2008-2013* (*Cybersecurity Strategy 2008-2013*), Tallinn, Estonia: Kaitseministeerium, The Ministry of Defense, 2008, available from *https://www.riigikantselei.ee/valitsus/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf*, accessed on February 9, 2014.

17. Ministry of Economic Affairs and Communications/ Department of State Information Systems, Information Security Interoperability Framework, Version 2, December 22, 2011, available from *www.riso.ee/sites/default/files/koosvoime/security-framework.odt*, accessed on September 2, 2014.

18. Department of State Information Systems, Estonian Interoperability Framework, RISO.ee, available from *www.riso.ee/en/estonian-interoperability-framework*, accessed on September 2, 2014.

19. John Bumgarner and Scott Borg, *The* [United States Cyber Consequences Unit] *U.S.-CCU Cyber-Security Check List,* The U.S. Cyber Consequences Unit, usccu.us, 2007, available from *www.usccu.us/documents/US-CCU%20Cyber-Security%20Check%20List%202007.pdf*, accessed on September 5, 2014.

20. Supervisory Control and Data Acquisition, London, UK: Centre for the Protection of National Infrastructure, available from *www.cpni.gov.uk/scada,* accessed on September 2, 2014.

21. *Infosüsteemide turvameetmete süsteem ISKE* (Information Systems Security System ISKE), Riigi Infosüsteemi Amet, available from *https://www.ria.ee/ee/index.php?id=33279*, accessed on September 5, 2014.

22. *ISKE Rakendusjuhend v. 7.00* (ISKE Implementation Guide, Version 7.00), Riigi Infosüsteemi Amet, March 2014, available from *https://www.ria.ee/public/ISKE/iske_rakendusjuhend_7_00.pdf*, accessed on September 2, 2014.

23. *ISKE Kataloogid v. 7.00* (ISKE Directories, Version 7.00), February 2014, Riigi Infosüsteemi Amet, available from *https://www.ria.ee/public/ISKE/ISKE_kataloogid_ver_7.00.pdf*, accessed on September 2, 2014.

24. *Andmekeskuse Turvanouded* (*Data Center Security Requirements*), Riigi Infosüsteemi Amet, April 2014, available from *https://www.ria.ee/public/KIIK/AndmekeskuseTurvanouded.pdf*, accessed on September 2, 2014.

25. *Kruptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring, Versioon 3.1* (New Cryptographic Algorithms, Uses and Life Cycle Study, Version 3.1), Riigi Infofüfteemi Amet, December

31, 2013, available from *https://www.ria.ee/public/PKI/kruptograafiliste_algoritmide_elutsukli_uuring_II.pdf*, accessed on September 2, 2014.

26. CERT Estonia, Estonian Information System Authority, available from *https://www.ria.ee/cert-estonia/*, accessed on September 2, 2014.

27. Clarified Networks Oy is a Codenomicon Group Company; see *https://www.clarifiednetworks.com/*, accessed on September 2, 2014.

28. Press Release 2011-05-23, Munich, Germany: Codenomicon Ltd, May 23, 2011, available from *www.codenomicon.com/news/press-releases/2011-05-23.shtml*, accessed on September 2, 2014.

29. Virtual Situation Room - VSR, Riigi Infosüsteemi Amet, available from *https://www.ria.ee/vsr/*, accessed on September 2, 2014.

30. Lauri Pokka and Sebastian Turpeinen, "Virtual Situation Room (Clarified VSRoom)—A Situation Awareness System for Critical Infrastructure," Munich, Germany: Clarified Networks Oy, December 27, 2011, available from *https://www.clarifiednetworks.com/Clarified%20VSRoom*, accessed on September 2, 2014.

31. *Estonian Defence League.* Tallinn, Estonia: Kaitseliit, September 19, 2014, available from *www.kaitseliit.ee/en/edl*, accessed on September 19, 2014.

32. *The Main Tasks of the EDL CU,* Tallinn, Estonia: Kaitseliit, September 19, 2014, available from *www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu*, accessed on September 19, 2014.

33. "Thousands Flee Dresden Floods," *The Guardian*, August 16, 2002, available from *www.theguardian.com/world/2002/aug/16/naturaldisasters.weather*.

34. *Grundgesetz Art. 62, Bundesministerium der Justiz und für Verbraucherschutz* (Constitution Article 62, Federal Office of Justice and Consumer Protection), available from *www.gesetze-im-internet.de/gg/art_62.html,* accessed on July 30, 2014.

35. *Grundgesetz Art. 65, Bundesministerium der Justiz und für Verbraucherschutz,* (Constitution Article 65, Federal Office of Justice and Consumer Protection), available from *www.gesetze-im-internet.de/gg/art_65.html*), accessed on July 30, 2014; *Grundgesetz Art. 65a, Bundesministerium der Justiz und für Verbraucherschutz* (Constitution Article 65a, Federal Office of Justice and Consumer Protection), available from *www.gesetze-im-internet.de/gg/art_65a.html*, accessed on July 30, 2014.

36. Christian Kahl, Nachrichten, Vom Kampf in der fünften Dimension (News - Battle in the fifth dimension), *Bundeswehr-Journal* (*German Federal Armed Forces-Journal*), May 3, 2013, available from *www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension/*, accessed on July 30, 2014; "Digitaler Truppeneinsatz: Bundeswehr meldet sich bereit zum Cyberwar" ("Digital Task Force: The Federal Armed Forces Are Prepared for Cyberwar"), *Spiegel Online*, June 5, 2012, available from *www.spiegel.de/netzwelt/netzpolitik/cyberwar-die-bundeswehr-kann-nun-auch-cyberkrieg-a-836991.html*, accessed on July 30, 2014.

37. Christoph Streiß, *Das Trennungsgebot zwischen Polizei und Nachrichtendiensten: Im Lichte aktueller Herausforderungen des Sicherheitsrechts* (*The Separation Requirement between Police and Intelligence Services: Under the Light of Current Challenges of Security Law*), Frankfurt, Germany: Peter Lang, 2011.

38. *Bundesministerium des Inneren* (hereafter BMI), *Umsetzungsplan KRITIS - des Nationalen Plans zum Schutz kritischer Infrastrukturen* (Implementation Plan KRITIS of the National Plan for the Protection of Critical Infrastructures), 2007, available from *www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile*, accessed on July 30, 2014; Artikelnummer: BMI07310.

39. BSI, UP KRITIS, available from *https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/Umsetzungsplan/umsetzungsplan_node.html*, accessed on July 30, 2014.

40. BMI, KRITIS Strategie (KRITIS Strategy), June 17, 2009, available from *www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile*, accessed on July 30, 2014, Artikelnummer: BMI09324.

41. BMI, *Nationaler Plan zum Schutz der Informationsinfrastrukturen, NPSI,* (National Plan for the Protection of Information, NPSI), available from *www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf*, accessed on July 30, 2014.

42. See *www.kritis.bund.de/SubSites/Kritis/EN/strategy/strategy_node.html*.

43. BMI, *Cybersicherheitsstrategie*, (*Cybersecurity Strategy*), available from *www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?_blob=publicationFile*, accessed on July 30, 2014.

44. Information throughout this section is drawn from BMI, *Nationales Cyber-Abwehrzentrum* (National Cyber Defense Center). BMI, 2014, available from *www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html*, accessed on July 30, 2014.

45. For example, these references occur in media reporting of a "*Bericht zum Themenkomplex*" (reports on topics of cyberwarfare), presented in 2012 to the Defense Committee by (then) Defense Minister Thomas Kossendey. See *www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension/*.

46. "*Spionage- und Hackerabwehr: Bundeswehr baut geheime Cyberwar-Truppe auf*" ("Defense of Espionage and Hacking: Fedeeral Armed Forces Builds Secret Troop against Cyberwar"), *Spiegel Online*, February 7, 2009, available from *www.spiegel.de/netzwelt/tech/spionage-und-hackerabwehr-bundeswehr-baut-geheime-cyberwar-truppe-auf-a-606096.html*, accessed on July 30, 2014..

47. See *www.amprion.de/en/portrait*.

48. BMI, available from *www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cybersicherheitsrat/cybersicherheitsrat_node.html*, accessed on July 30, 2014.

49. BSI, *IT-Grundschutz-Kataloge* (Baseline Protection Catalogs), available from *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html*, accessed on July 30, 2014.

50. BSI, *Bausteine* (Blocks), available from *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Bausteine/bausteine_node.html*, accessed on July 30, 2014.

51. BSI, *Gefährdungskatalog* (Measures Catalog), available from *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Gefaehrdungskataloge/gefaehrdungskataloge_node.html*, accessed on July 30, 2014.

52. BSI, *Maßnahmenkatalog* (Action Plan Catalog), available from *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/massnahmenkataloge_node.html*, accessed on July 30, 2014.

53. BSI, *Grundschutzkatalog* (Baseline Protection Catalogs), 2013, available from *https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf*, accessed on July 30, 2014.

54. BSI, *Bürger*-CERT, available from *https://www.buerger-cert.de/*, accessed on July 30, 2014.

55. BSI, BSI *für Bürger* (BSI for Citizens), available from *https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html*, accessed on July 30, 2014.

56. BSI, *IT-Lagezentrum* (IT Situation Center), available from *https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Lagezentrum/itlagezentrum_node.html*, accessed on July 30, 2014.

57. BSI, Organisations Plan, April 2014, available from *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/Organisationsplan_IFG_pdf.pdf?__blob=publicationFile*, accessed on July 30, 2014.

58. BSI, CERT-*Bund*, available from *https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/CERTBund/certbund_node.html*, accessed on July 30, 2014.

59. See *www.y-punkt.de/portal/a/ypunkt/!ut/p/c4/LYvBCsIwEAX_aLdBKuqtNRevvWi9SNosJTRNwrKxCH68CfgG5jI8fGIhmLdbjLgYjMcHjrO7TDtMu6XXJ-WwCphVMnkPwjklwnt9WYI5BpJqoSCueGEjkSFFFl9LZi4FnMWxUbpXB9X8p77n61G33alt9K0fMG1b9wMz70k0/*; see also *www.tagesspiegel.de/politik/soldaten-ausbildung-fuer-den-cyberwar-die-abwehr-abteilung-der-bundeswehr-zaehlt-rund-800-attacken-im-jahr/8223514-2.html*.

60. Anonymous interview with German official, August 2014.

61. Computer-Emergency-Response-Team der Bundeswehr, available from *www.bundeswehr.de/portal/a/bwde/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pPKUVL2y1K-LyxJyS0rx0vcTS4qLS1GIQOz4zLy0_Pq-0pAokkZxaVJJUrl-Q7agIA-PDk_Ls!/*, accessed on July 30, 2014; *Bundesamt für Austrüstung, Informationstechnik und Nutzung der Bundeswehr* (Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, Business Division 100, November 26, 2013, accessed on July 30, 2014; see also *www.baain.de/portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy9lM-zUvOKSYr3MkiqgWH5RemJeZjFYrV56kqGBgX5BtqMiAGrZfXo!/* . Sarah Kramer, *Der Tagesspiegel*, *Im Schützengraben der IT-Krieger* (In the Trench of IT Warriors), May 20, 2014, available from *www.tagesspiegel.de/politik/soldaten-ausbildung-fuer-den-cyberwar-die-abwehr-abteilung-der-bundeswehr-zaehlt-rund-800-attacken-im-jahr/8223514-2.html*, accessed on July 30, 2014.

62. *Bundeskriminalamt* (BKA) - *Stellenangebote*, *Administrator im Bereich zentrale Unternehmensserver (Administrator for Central Business Servers),* 2014, available from *www.bka.de/nn_246784/DE/Berufsperspektive/Stellenangebote/17-2014,templateId=raw,property=publicationFile.pdf/17-2014.pdf*, accessed on July 30, 2014.

63. *Bundesverwaltungsamt* (BVA), *Stellenausschreibung - Referent/Referentin im Referat Chip-Sicherheitsanalyse (Job Offers: Advisor for the Chip Security Server Analytics),* 2014, available from *www.bva.bund.de/SharedDocs/Stellenangebote/DE/DLZ/040_HoehererDienst/BSI_2014_038_22082014.html*, accessed on July 30, 2014.

64. Linda Vespestad and Elin Fossum, NRK - *Norsk rikskringkasting* AS (The Norwegian Broadcasting Corporation, hereafter NRK), *Forsvaret øker innsatsen mot datahackere med Cyberforsvaret* (*The Defense [Norwegian Armed Forces] Increases Efforts against Hackers with Cyber Force*), September 18, 2012, available from *www.nrk.no/ho/okt-forsvarsinnsats-mot-datahackere-1.8326973*, accessed on July 15, 2014.

65. *Nasjonala Sikkerhetsmyndigheten*, ("The National Security"), available from *https://www.nsm.stat.no/*, accessed on July 15, 2014.

66. Sveinung Berg Bentzrod, "Ny militär gren cyberspaceforsvar," ("New Military Branch Cyberspace Defense"), *Aftenposten*, October 12, 2011, available from *www.aftenposten.no/nyheter/Ny-militar-gren-cyberspaceforsvar-5331697.html#.U87BrrE385o*, accessed on July 15, 2014.

67. See *www.regjeringen.no/nb/dep/fd/dok/regpubl/prop/2011-2012/prop-73-s-20112012/7/8/3.html?id=676153*.

68. Tale Sundlisæter, Teknisk Ukeblad. *Forsvarets cyberkonferanse 2013 forbereder Norge pa cyberangrep.* (*The Norwegian Cyberconference, 2013, Prepared Norway for Cyberattacks*), April 23, 2013, available from *www.tu.no/industri/2013/04/23/forbereder-norge-pa-cyberangrep*, accessed on July 15, 2014.

69. See *www.regjeringen.no/nb/dep/fd/dok/regpubl/prop/2011-2012/prop-73-s-20112012/7/8/3.html?id=676153*.

70. Center for Cyber and Information Security, available from *https://ccis.no/about-ccis/*, accessed on July 15, 2014.

71. Center for Cyber and Information Security brochure (English version), 2013, available from *ccis.no/wp-content/uploads/2014/06/CCIS-brosjyre-2014-English-.pdf*, accessed on July 15, 2014.

72. Nasjonala Sikkerhetsmyndigheten, *Organisasjon* (National Security Authority, hereafter, NSM), available from *https://www.nsm.stat.no/Om-NSM/Organisasjon/*.

73. NSM, *Rapport om sikkerhetstilstanden* (*Report on the Security*), available from *https://www.nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/)*, accessed on July 10, 2014.

74. NSM, *Varslingssystem for digital infrastruktur (Warning System for Digital Infrastructure)*, available from *https://www.nsm.stat.no/tjenester/varslingssystem-for-digital-infrastruktur-vdi/*, accessed on July 15, 2014.

75. NRK.

76. Sigvald Sveinbjørnsson, DIGI.no - *IT-bransjens nettavis* (IT Industry News Site), *"NRK kastet ut statens 'spionboks'"* (NRK Evicted State 'Spy Box'"), November 5, 2012, available from *www.digi.no/905476/nrk-kastet-ut-statens-spionboks*, accessed on July 15, 2014.

77. *Norsk Center for Informasjonssikring* (Norwegian Center for Information Security) available from *https://norsis.no/om-norsis/*, accessed on July 15, 2014.

78. Kristian Ervik, *Norges cyberforsvar: – Vi utsettes daglig for inntrengningsforsøk* (*Norway's Cyber Defense: We Are Exposed Daily to Intrusion*), February 21, 2013, available from *www.tv2.no/a/3993983*, accessed on July 15, 2014.

79. IKT Nytt (ICT News), available from *iktnytt.no/kyberkrig-kybersikkerhet/*; Jonas Blich Bakken, Dagens Naeringsliv, *Vår svakeste forsvarsgren: - Vi opplever målrettede angrep, hver uke* (Our Weakest Military Branch: We Are Experiencing Targeted Attacks), February 23, 2013, available from *www.dn.no/tekno/2013/02/23/var-svakeste-forsvarsgren-vi-opplever-malrettede-angrep-hver-uke*, accessed on July 15, 2014.

80. Larsen-Vonstett, Oystein. VG.no. *Sikkerhetsekspert: Nordmenn er naive!* ("Security Expert: Norwegians Are Naive"), June 17, 2012, available from *www.vg.no/nyheter/innenriks/datasikkerhet/sikkerhetsekspert-nordmenn-er-naive/a/10058063/*, accessed on July 15, 2014.

81. *Försvarsdepartments Myndigheter* (*The Government: Authorities of the Royal Norwegian Ministry of Defense),* May 23, 2013, available from *www.regeringen.se/sb/d/495/a/3174*, accessed on January 7, 2014.

82. Filip (Philip) Struwe, SVT.se, *FRA lagrar svenska telesamtal och mejl* (*FRA Stores Swedish Telephone Calls and E-mails*), June 16, 2008, available from *www.svt.se/nyheter/sverige/fra-lagrar-svenska-telesamtal-och-mejl*, accessed on July 1, 2014.

83. Henrik Hedberg and Jesper Gyberg, Regeringen.se. *Pressmedelande: Sverige får nytt signalspaningsfartyg* (*Press Release. Sweden Gets New Signals Intelligence Gathering*), April 22, 2010, avail-

able from *www.regeringen.se/sb/d/12760/a/144452*, accessed on July 1, 2014.

84. *Förslag till statens bugdet för 2014: Försvar och samhällets krisberedskap* (*Draft on State Budget 2014: Defense and Emergency Preparedness*), Regeringen.se, available from *www.regeringen.se/content/1/c6/11/17/88/f1fdc12f.pdf*, accessed on July 1, 2014; PROP 2013/14:1 Utgiftsomrade 6 (Category 6).

85. *Arsöversikt 2012 Militära Underrättelse- och Säkerhetstjänsten*, (*Annual Review 2012, Military Intelligence and Security*), Stockholm, Sweden: Försvarsmakten, 2012. ProdID 130508-003.

86. *Försvarsmaktens säkerhetstjänst, informationsionssäkerhet* (*The Armed Forces Security Service, Information Security*), Stockholm, Sweden : Försvarsmakten, 2013. M7739-352056.

87. Niklas Dahlin and Monica Kleja, "*Spionvirus hot mot Sverige*" ("*Spy Virus Threat to Sweden*"), NyTeknik, December 5, 2012, available from *www.nyteknik.se*, accessed on July 1, 2014.

88. *Pressmedelande: Bristande kännedom hos Försvarsmakten om risker av användning av sociala medier* (*Press Release: Lack of Awareness of the Armed Forces on the Risks of Using Social Media*), FOI.se, December 19, 2013, available from *www.foi.se/sv/nyheter/Press--nyheter/Nyheter/2013/Bristande-kannedom-i-Forsvarsmakten-om-risker-av-anvandning-av-sociala-medier-/*, accessed on July 1, 2014; Henrik Karlzén, *Användning av socialer medier i Försvarsmakten* (*The Use of Social Media by the Armed Forces*), Stockholm, Sweden : Totalförsvarets foskningsinstitut, 2013, available from *FOI-R--3674--SE*.

89. *Pressmedelande: Tar datorn till rätt säkerhetsnivå* (*Press Release: Bringing the Computer to the Right Security*), FOI.se, December 11, 2013, available from *www.foi.se/sv/nyheter/Press--nyheter/Nyheter/2013/Tar-datorn-till-ratt-sakerhetsniva/*, accessed on July 1, 2014.

90. Peter Stenumgaard, *Störningskänslighet hos civil trådlös konsumentteknik* (*Sensitivity of Civilian Wireless Consumer Technology to Disturbances*), Linköping, Sweden: Totalförsvarets foskningsinstitut, 2012, available from *FOI-R--3216--SE*.

91. "*Bildt Defends Sweden Surveillance*," *The Local*, November 3, 2013, available from *www.thelocal.se/20131103/bildt-defends-sweden-surveillance*.

92. Anonymous interview with German official, August 2014.

93. "Defence Minister: Police and Defence Forces to Get Wider Web Powers," *YLE News*, November 2, 2013, available from *yle.fi/uutiset/defence_minister_police_and_defence_forces_to_get_wider_web_powers/6914546*.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

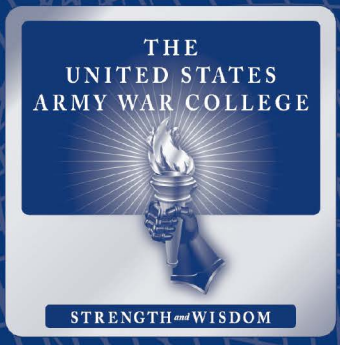
Author
Mr. Keir Giles
Ms. Kim Hartmann

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Jennifer E. Nevil



FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

ISBN 1-58487-697-2

This Publication

SSI Website

USAWC Website