



REPORT

PREPARING FOR CYBER CONFLICT

CASE STUDIES OF CYBER COMMAND

| PIRET PERNIK |

DECEMBER 2018

RKK
ICDS

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: Preparing for Cyber Conflict: Case Studies of Cyber Command

Author: Pernik, Piret

Publication date: December 2018

Category: Report

Cover page photo: Computer racks, by Tristan Schmurr on Flickr, made available under an Attribution 2.0 Generic (CC BY 2.0) license (<https://creativecommons.org/licenses/by/2.0/legalcode>) and used without any changes

Other photos used in the report:

Page V – A padlock is displayed at the Alert Logic booth during the 2016 Black Hat cyber-security conference in Las Vegas, Nevada, U.S. August 3, 2016. REUTERS/David Becker

Page 38 – 1Lt Michael Newman looks over a rack in the server room at the Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado Springs

Keywords: Cyber Command, Offensive Cyberspace Capabilities, Armed Forces, Cyber Defence, Operational Planning

Disclaimer: The views and opinions contained in this report are solely those of its author and do not necessarily represent the official policy or position of the International Centre for Defence and Security or any other organisation.

ISSN 2228-0529

ISBN 978-9949-7255-7-1 (print)

ISBN 978-9949-7255-8-8 (PDF)

©International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

ACKNOWLEDGEMENTS

I am very grateful to all my colleagues for the support and valuable suggestions they provided during the drafting of this study; in particular, I would like to thank the following subject matter experts, with the caveat that final responsibility for any errors presented here remains of course my own: Christian Marc Lifländer, Kristin Hemmer Mørkestøl, Matthijs Veenendaal, Mano Nokelainen, Mika Kerttunen, Siim Alatalu, Andrus Padar, Rain Ottis, Tiia Sõmer, Stephan Michael Lissinna, Christian Hetsch, Patrick Jungkunz, Silver Andre, Uko Valtenberg, Tony Lawrence, and Emmet Tuohy.

ABOUT THE AUTHOR

Piret Pernik joined the International Centre for Defence and Security in April 2013. Her research focuses on cyber security policy-making and other strategic issues relevant to cyber security. Her tasks include analysing global developments, including strategies and policies pursued by states and international organisations. She recommends how to shape Estonia's efforts on cyber security and on how to introduce the Estonian experience internationally, as well as coordinates cyber security related cooperation with other relevant domestic and international actors.

Before joining ICDS, she worked at the Policy Planning Department of the Estonian Ministry of Defence (in 2003–2009 and in 2012–2013). In 2009–2012, she served as an adviser to the National Defence Committee of the Riigikogu (Estonian Parliament). Piret Pernik has studied sociology at the Estonian Humanitarian Institute and political science at the University of Tartu. She holds a Master's degree in Sociology, and a Master's degree in International Relations and European Studies from Central European University in Budapest.

EXECUTIVE SUMMARY

This is the first publicly available comparative study of the military cyber organisations in five European countries: Estonia, Finland, Germany, the Netherlands, and Norway.¹ The study examines strategic guidelines, political authorisation of international deployments, organisational set-up, the chain of command, and key functions of three categories of military cyberspace forces: cyber commands (Estonia, the Netherlands, Norway), military cyber services (Germany), and cyber defence divisions (Finland). The second part discusses rationales for the establishment of each specific organisational set-up, and considers the advantages and disadvantages of these different models. The last section presents policy recommendations in these areas (political authorisation, organisation, chain of command, functions).

¹ These organisations are: cyber commands in Estonia, in the Netherlands, and in Norway; cyber military service in Germany and cyber defence division in Finland.

LIST OF ABBREVIATIONS

AIVD	<i>Algemene Inlichtigen- en Veiligheidsdienst</i> (General Intelligence and Security Service, Netherlands)
BfV	<i>Bundesamt für Verfassungsschutz</i> (Federal Office for the Protection of the Constitution, Germany)
BKI	<i>beskyttelse av kritisk infrastruktur</i> (Computer Emergency Response Team of the Armed Forces of Norway)
BND	<i>Bundesnachrichtendienst</i> (Federal Intelligence Service, Germany)
C2	Command and Control
C5	Command, Control, Communications, Computers, Cyber
C5 Agency	<i>Puolustusvoimien johtamisjärjestelmakeskus</i> (Finnish Defence Forces C5 Agency)
CDU	Cyber Defence Unit of the Estonian Defence League
CERT	Computer Emergency Response Team
CERTBw	Bundeswehr Computer Emergency Response Team
CHoD	Chief of Defence
CIR	<i>Organisationsbereich Cyber- und Informationsraum</i> (Cyber and Information Domain Service, Germany)
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
CIS	Communication and Information Systems
Cyber Defence	<i>Cyberforsvaret</i> (Norwegian Armed Forces Cyber Defence)
DefCERT	<i>Defensie Computer Emergency Response Team</i> (Netherlands Armed Forces Computer Emergency Response Team)
E-tjenesten	<i>Etterretningstjenesten</i> (Norwegian Intelligence Service)
ICT	Information and Communication Technology
ISR	Intelligence, Surveillance, Reconnaissance
IT	Information Technology
InspCIR	<i>Inspekteur</i> (Chief of Cyber and Information Domain Service, Germany)
J6	Command, Control, Communications, Computers, Cyber Directorate
JSCU	Joint Signal Intelligence Unit, Netherlands
KdoCIR	<i>Das Kommando Cyber- und Informationsraum</i> (Headquarters of Cyber and Information Domain Service, Germany)
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
NCAZ	<i>Nationales Cyber-Abwehrzentrum</i> (National Centre for Cyber Defence, Germany)
NCSC	National Cyber Security Centre, Netherlands
NSM	<i>Nasjonal sikkerhetsmyndighet</i> (Norwegian National Security Authority)
MIVD	<i>Militaire Inlichtingen- en Veiligheidsdienst</i> (Military Intelligence and Security Service, Netherlands)
PVTIEDL	<i>Puolustusvoimien tiedustelulaitos</i> (Finnish Defence Intelligence Agency)
SSB	Support and Signal Battalion, Estonia
SUPO	<i>Suojelupoliisi</i> (Finnish Security Intelligence Service)
TTTP	Tools, tactics, techniques and procedures
USCYBERCOM	United States Cyber Command



INTRODUCTION

Although armed forces began to build their own cyber capabilities as early as the 1990s, it took longer for the first full-fledged cyber command to emerge; the United States Cyber Command (USCYBERCOM) achieved initial operational capability only in 2010 and full operational capability in September 2018.² Thus despite much media hype about a “cyber arms race,” the development of military cyber forces has been an incremental process, one that has taken place over several decades.

By now at least eight other NATO allies have created standalone cyber commands or services within their armed forces: Estonia, France, Germany, Italy, the Netherlands, Norway, Spain, and Turkey. In October 2018, Estonia, Denmark, the Netherlands, the United Kingdom and the United States announced that they would contribute national cyberspace forces to NATO missions and operations.³ In many NATO countries, (e.g. US, France, Germany, Spain, the Netherlands, and Estonia), the authorities have disclosed that they are developing offensive cyberspace capabilities in their armed forces. In addition, a number of countries possess offensive cyberspace capabilities in their military intelligence services – for example, Australia, Belgium, the Czech Republic, Denmark, Finland, Norway, and the UK.⁴ Furthermore, civilian signal intelligence services in several countries also possess their own offensive

capabilities – for example, those of the US, UK, the Netherlands, and Canada.⁵ Hence, there are a myriad of offensive cyberspace capabilities being developed by NATO allies within civilian intelligence services and the armed forces alike.

However, at the same time, the visions, missions, mandates, functions, and capabilities of cyber forces across these countries vary. Despite these differences, the armed forces themselves frequently refer to all types of cyber forces as “cyber commands.” There is no common understanding of what constitutes a cyber command nor a comprehensive overview of the existing military cyberspace forces. As the first publicly available comparative analysis of military cyberspace organisations– focusing on five European countries: Estonia, Finland, Germany, the Netherlands, and Norway– this study seeks to fill this gap.⁶

There is no common understanding of what constitutes a cyber command nor a comprehensive overview of the existing military cyberspace forces

It examines the strategic guidelines, political authorisation of international deployments, organisational set-up and the chain of command, and key functions of three categories of military cyberspace forces: cyber commands (Estonia, the Netherlands, Norway), military cyber services (Germany), and cyber defence divisions (Finland). All the selected countries except Norway are EU member states, and all except Finland are NATO allies. Moreover, all except

² Jason Healy, ed., *A Fierce Domain: Conflict in Cyberspace: 1986 to 2012*, Part I (Arlington, VA: Cyber Conflict Studies Association, 2013). In spring 2018 USCYBERCOM was elevated from a sub-unified command to a unified combatant command subordinated to the Secretary of Defence. The full operational capability consists of 6,200 military and civilian personnel. See “US Cyber Command History,” US Cyber Command, <https://www.cybercom.mil/About/History> (accessed November 2, 2018).

³ “News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium,” US Department of Defence, October 4, 2018, <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/> (accessed November 2, 2018).

⁴ All of these states except Denmark have publicly confirmed the development of such capabilities.

⁵ South Korea and India have created cyber commands. Colombia and Vietnam have also cyber commands, but thus far have not signalled an intention to develop offensive capabilities. In Singapore the C4 Operations Group of the Singapore Armed Forces (SAF) Headquarters’ C4 Command implements cyber defence operations and capabilities. It is thus technically not a standalone cyber command. See “Fact Sheet: SAF C4 Command Integrates C4 and Cyber Defence Capabilities,” Ministry of Defence of Singapore, June 30, 2017, <https://www.mindef.gov.sg> (accessed October 9, 2018). It is believed that Belgium, Colombia and United Arab Emirates possess offensive cyberspace capabilities, but public authorities of these countries have not confirmed the development of offensive capabilities; if they do exist, it is not known in which organisation they reside. See Max Smeets, Herbert Lin, “Offensive Cyberspace capabilities: To What Ends?,” in T. Minarik, et. al (eds.), *10th International Conference on Cyber Conflict. CyCon X: Maximising Effects* (Tallinn: NATO CCD COE Publications, 2018), pp. 55-72.

⁶ These organisations are: cyber commands in Estonia, the Netherlands, and Norway; the cyber military service in Germany, and the cyber defence division in Finland.

one (Germany) of the countries included in this study are small in size, while each of them has demonstrated advanced national-level cyber security and intelligence capabilities.

The study is structured into three chapters. The first explains key concepts and ideas related to cyberspace, cyberspace operations and the armed forces while providing definitions that are used throughout the document. Based on empirical primary-source research (official strategic documents and government websites) and interviews with national subject matter experts, the second chapter consists of five national case studies and examines the strategic guidelines, political authorisation of international deployments, organisational set-up and the chain of command, and key functions with regard to each country. Finally, the third chapter presents in-depth analysis of the study's key findings, including policy recommendations in these areas.

1. TERMINOLOGY

In this study, the terms “cyber capabilities” and “cyber operations” are used synonymously and interchangeably with “cyberspace capabilities” and “cyberspace operations.” The concepts of “cyberspace” and the “cyber domain” are used similarly, though the latter specifically refers to cyberspace as a domain for military operations. In this study the term Computer Incident Response Capability (CIRC) is defined as “a capability set up for the purpose of assisting in responding to computer security-related incidents” and is used synonymously with the following: Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT).⁷

1.1. CYBERSPACE OPERATIONS

According to a NATO International Military Staff working document of 15 March 2018, the Alliances cyberspace operations fall into four categories:

- 1) Communication and Information Systems (CIS) Infrastructure Operations (passive measures of prevention, protection, and recovery),

- 2) Defensive Cyberspace Operations (active measures of detection and reaction),
- 3) Intelligence, Surveillance, Reconnaissance (non-intrusive and intrusive intelligence collection; operational preparation of the environment),
- 4) Offensive Cyberspace Operations (denial and manipulation operations, operational preparation of the environment).⁸

In this study, for simplification the first category is merged into the second, as both are undertaken either in one's own or in friendly networks for defensive purposes.⁹ Accordingly, throughout the current document there are three main categories of cyberspace operations:

- 1) Defensive cyberspace operations;
- 2) Intelligence, surveillance, reconnaissance (ISR) cyberspace operations;
- 3) Offensive cyberspace operations.¹⁰

These categories will be further explained in the following paragraphs.

It is widely accepted that effective cyber defence requires integrating offensive capabilities into defensive operations, whose purpose is defending one's own as well as friendly networks (in military and cybersecurity terminology, known as “blue networks.”)¹¹ Even though they are called “defensive” operations they can encompass offensive activities at the

⁸ Javier López de Turiso y Sánchez, “Evolución del Concepto de Ciberdefensa,” Military Operations in Cyberspace: The Third Cyber Defence Symposium of the Spanish Joint Cyber Defence Command (Madrid, May 24, 2018), p. 38, <https://jornadasciberdefensa.es/2018/programa/255/es> (accessed October 10, 2018).

⁹ This categorisation is consistent with the threefold categorisation of cyberspace operations into defensive, exploitation and attack operations in NATO's AAP-6. A computer network attack (in this paper offensive cyberspace operation) is an action taken to disrupt, deny, degrade, destroy information resident in a computer and network, or the computer and network itself. Computer network exploitation (in this paper ISR cyberspace operation) is an action to make use of computer, network and/or information therein to gain advantage. See *NATO Glossary of Terms and Definitions (English and French)*, AAP-06 (2017), edition 2017, (Brussels: North Atlantic Treaty Organisation, 2017).

¹⁰ This study uses the US Joint Chiefs of Staff definition of cyberspace operations: “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.” Source: Joint Chiefs of Staff, “Cyberspace Operations,” Joint Publication (JP) 3-12, June 8, 2018, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930 (accessed October 9, 2018).

¹¹ Paul McKenzie, *NATO Joint Air Power and Offensive Cyberspace operations*, Kalkar: Joint Air Power Competence Centre, November 2017, https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf (accessed November 10, 2018).

⁷ Paul Cichonski et al, *Computer Security Incident Handling Guide* (Gaithersburg, MD: National Institute of Standards and Technology, August 2012), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (accessed November 5, 2018).

operational and technical level, though the purpose of these offensive activities is still defending blue networks from active threats and/or from a specific adversary.¹²

Defensive cyberspace operations can be executed in the networks of adversaries (“red networks”) and of third parties (“grey networks”).¹³ Therefore the key difference between defensive cyberspace operations and the two other categories used in this study is that the former are executed for the purposes of protection and defence, while by contrast the objectives of ISR cyberspace operations and offensive cyberspace operations are, respectively, intelligence collection and projecting power in and through cyberspace.¹⁴

Offensive cyberspace operations create “first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 [Command and Control] processes, logistics nodes, high-value targets, etc.”¹⁵ In contrast, although ISR cyberspace operations also normally require intrusions into grey and red networks, the purpose is not to achieve cyber effects, but is

instead intelligence collection. Both defensive and offensive operations may include actions that rise to the level of the use of force, and may result in physical damage to – or even the destruction of – an adversary’s systems.¹⁶

1.2. CYBERSPACE EFFECTS

In military terminology, the concept “cyberspace effects” (or, more specifically, defensive cyberspace effects and offensive cyberspace effects) are commonly used to describe the range of consequences of cyberspace operations. Cyberspace effects are defined in this study as “the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.”¹⁷ According to some conceptualisations, these effects can also be in the cognitive domain.¹⁸

1.3. CYBER COMMAND

There is no commonly agreed definition of the term “cyber command.” It generally denotes a standalone command structure, branch or service of the armed forces that directs and controls the three main categories of cyberspace operations described above. The best example is USCYBERCOM.¹⁹

However, both military and media sources commonly use the term more broadly to denote any type of military cyber defence organisation, without any reference to their exact mandate or capabilities – especially the authority to direct and control the full spectrum of cyberspace operations. In

Both defensive and offensive operations may include actions that rise to the level of the use of force, and may result in physical damage to – or even the destruction of – an adversary’s systems

¹² If these operations encompass activities outside blue networks, the US calls them “Defensive Cyberspace Operations Response Actions.” See “Cyberspace Operations,” II-4.

¹³ For example, the US Army conducts three types of cyberspace missions: Department of Defence information network (DODIN) operations, defensive cyberspace operations, and offensive cyberspace operations. “Defensive Cyberspace Operations Response Actions” are employed in response to specific threats, and may result in effects outside DODIN networks. See Headquarters Department of the Army, “Cyber Electromagnetic Activities,” FM 3-38, February 12, 2014, p. 8, <https://fas.org/irp/doddir/army/fm3-38.pdf> (accessed October 10, 2018). See also US Army Training and Doctrine Command (TRADOC), “The U.S. Army Concept for Cyberspace and Electronic Warfare Operations (2025-2040),” Pamphlet (TP) 525-8-6, January 9, 2018, <http://adminpubs.tradoc.army.mil/pamphlets.html> (accessed October 10, 2018) and “Cyberspace Operations” p. xi.

¹⁴ There exist many conceptions of the continuum between passive and active cyberspace operations, but in general, passive activities are those executed in friendly systems, while active activities are those undertaken outside these systems.

¹⁵ “Cyberspace Operations,” II-5.

¹⁶ “Cyberspace Operations,” II-5.

¹⁷ This definition does not extend to include defensive cyberspace effects. See “Cyber Electromagnetic Activities,” p. 9-10.

¹⁸ Hans Folmer, „Demystifying Cyber Operations,” Ministry of Defence, Netherlands Military Law Review, https://puc.overheid.nl/mrt/doc/PUC_248329_11/1/ (accessed November 5, 2018).

¹⁹ USCYBERCOM’s support to combatant commanders includes defensive, intelligence and offensive cyberspace operations. See “Cyberspace Operations,” II. USCYBERCOM forces are staffed, trained, and equipped to collect and report intelligence and information, and conduct cyberspace operations. See “Operation Glowing Symphony,” USCYBERCOM OPORD 16-0188, June 27, 2018, <https://www.documentcloud.org/documents/4624362-Cybercom-Operation-Glowing-Symphony-Documents.html> (accessed November 5, 2018).

practice many cyber commands do not fulfil all these functions, and the term is commonly used in the broader meaning of having the capability and authority to execute various cyber defence-related functions (for example, ICT security and services, CIS security, building cyber forces, etc.)

In three of the countries covered by this study—Estonia, the Netherlands, and Germany—military cyberspace organisations in the above narrower sense (independent entity with the capability and authority to direct and control defensive, ISR, and offensive operations) exist, although in the last example the organisation can be considered a hybrid of a combatant command and a military service.²⁰

In Estonia, the Netherlands, and Norway military cyberspace organisations are subordinated to the commanders of the defence forces (in NATO/EU terminology, a country's senior uniformed officer is referred to as the Chiefs of Defence, or CHoD); in Germany, by contrast, the military cyberspace organisation reports to the Ministry of Defence, and in Finland, the Cyber Division is subordinated to the C5 Agency of the Defence Forces' Headquarters and reports to the latter's chief.

Even though Norway has a branch of the armed forces called Cyber Defence, it does not constitute a cyber command in the above narrower sense because it directs and controls only defensive cyberspace operations, while offensive and ISR operations are directed and controlled by the Norwegian Intelligence Service subordinated to CHoD. Interestingly, Cyber Defence's role in protecting national critical infrastructure will expand in the next years (see more in the Norway case study below) which further highlights its competence in the civilian and private sectors.

1.4. ARMED FORCES

Because each country uses slightly different military terminology, to facilitate comparison general terms are used to refer to equivalent military organisations or positions outside the country case studies (where the official local names are used). The general terms "military," "defence forces," and "armed forces" are used synonymously in addition to official names such as "Estonian Defence Forces." In addition, the term "whole defence organisation" is used to refer to the administrative or governance area of the Ministry of Defence, including the armed forces and other agencies falling under this area. Some countries (for example, Finland) use the term "Commander of the Defence Forces" instead of the "Chief of Defence (CHoD)", but these terms are also used synonymously in this study. Similarly, "Defence Forces Headquarters" is used interchangeably with local terminology such as "General Staff", "Central Staff" (the Netherlands), and "Defence Command" (Finland).

Political authorisation of the deployment of offensive cyberspace capabilities refers to the political authority (for example, the parliament, government, president, or minister of defence) that decides on the military's use of force in and through cyberspace.

²⁰ In this study Germany's military cyberspace organisation is categorised as a standalone service, but in essence it constitutes a hybrid of a service and a combatant command because it fulfils the traditional role of military service in building and preparing the cyber forces and has command-like authorities to employ the forces in military operations, in cooperation with the Directorate General for Strategy and Operations.

2. CASE STUDIES

The following section will describe the missions, organisational structures, and key functions of cyber commands in Estonia, Finland, Germany, the Netherlands, and Norway. The information in this section is gathered primarily from open sources and includes government and armed forces strategies, doctrines, national legislation, websites, press articles and reports, and other sources. In addition, the author of this study conducted ten in-depth interviews with subject matter experts from the five countries.²¹ The information made publicly available by each country about its military cyber defence forces varies. Accordingly, the case studies differ in the level of detail about the specific functions and organisational setup in each country, reflecting the extent to which the author was able to collect relevant information.

2.1. ESTONIA: CYBER COMMAND

Strategic Guidelines

According to Cyber Security Strategy 2014-2017, Estonia is developing military cyber defence capabilities that include early warning, deterrence and active defence.²² Active defence usually refers to operations outside blue networks that are employed in response to specific threats.²³ In August 2018, the Estonian Defence Forces established Cyber Command, which will achieve full operational capability by 2023 and will consist of 300 military and civilian personnel, including professionals from the private sector.²⁴ Most of its workforce will be transferred from existing units; only

60 new positions will be created.²⁵ In addition, the Estonian Ministry of Defence includes a Cyber Policy and Information and Communications Technology (ICT) Department, subordinate to the Undersecretary for Legal and Administrative Affairs.²⁶

Rationale for Establishing Cyber Command

The pre-condition for establishing Cyber Command was the change of mindset of the military personnel. The Estonian experts interviewed hold that the founding of Cyber Command improves strategic and operational level commanders' understandings about the role of cyberspace operations in a kinetic conflict, allows them to understand the nature of cyberspace operations and become better aware of cyber threats to military missions and operations.²⁷

The founding of Cyber Command improves commanders' understandings about the nature of cyberspace operations and their role in a kinetic conflict

Political Authorisation of International Deployments

According to the National Defence Act, the parliament must decide to authorise each individual case of the use of the armed forces separately, unless the country is bound by treaty to participate in operations (such as NATO collective self-defence operation under the article 5 of the North Atlantic Treaty), or unless it has pre-authorised the use of Estonian components of armed rapid reaction forces prior to the start of their stand-by period within a rapid reaction force of NATO, the EU, or another ally.²⁸ In addition, the Estonian government can authorise defence readiness in the case of an

²¹ Interviews were conducted in December 2017 and February 2018 in Tallinn and Bonn with Kristin Hemmer Mørkestøl, Matthijs Veenendaal, Mano Nokelainen, Mika Kerttunen, Siim Alatalu, Andrus Padar, Rain Ottis, Tiia Sõmer, Stephan Michael Lissinna, Christian Hetsch, Patrick Jungkunz, Silver Andre, Uko Valtenberg.

²² Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017*, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (accessed November 5, 2018).

²³ See footnotes 11 and 12 for the definition of the term "Defensive Cyberspace Operations Response Actions."

²⁴ Ministry of Defence, "The National Defence Development Plan 2017-2026," <http://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/> (accessed November 5, 2018). Information System Authority, *Annual Cyber Security Assessment 2018*, page 32, <https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf> (accessed November 5, 2018).

²⁵ Mirjam Mäekivi, "Galerii: Eesti küberväejuhatuse asus tööle" [Gallery: Estonian Cyber Command Began Operating], *Eesti Rahvusringhääling (ERR)*, <https://www.err.ee/850643/galerii-eesti-kubervaejuhatuse-asus-toole> (accessed November 5, 2018).

²⁶ Ministry of Defence, last modified March 14, 2018, <http://www.kaitseministeerium.ee/en/organisation-contacts/ministry-defence>.

²⁷ Interviews conducted with Estonian experts in Tallinn, December, 2017.

²⁸ Parliament, "National Defence Act," passed on February 11, 2015, paragraph 33, <https://www.riigiteataja.ee/en/eli/ee/517112015001/consolide/current> (accessed November 5, 2018).

imminent threat to the security of the nation, or for participation in international military operations.²⁹ In this case, the armed forces can either fulfil national defence tasks that are established by legislation and provided for in the national defence action plan, or will be assigned additional tasks by the government. Accordingly, pursuant to the National Defence Act, offensive cyberspace operations can be deployed to support NATO and allied missions and operations without a prior decision of the *Riigikogu* (Estonian Parliament); however, a conclusive determination of the lawfulness of this possibility is beyond the scope of this study.³⁰

Mission

The mission of Cyber Command is to defend the information systems of the Estonian Defence Forces and of its allies while maintaining the readiness to conduct active cyber defence operations.³¹ According to a senior Ministry of Defence official, Cyber Command will be responsible for deterring and defeating threats to Estonian interests and infrastructures, defending the information environment of the Estonian Defence Forces, and providing mission assurance for military operations.³² Estonia is developing cyber capabilities with full regard for the interests and needs of NATO, and has declared its readiness to deploy offensive cyberspace capabilities in order to support missions and operations of the Alliance.³³

Organisation

Cyber Command, located in Tallinn, is one of the permanent structural units and wartime units of the Estonian Defence Forces (other such units are for example two infantry brigades, navy, air force, military police, etc.). Like the Norwegian cyber command, it is considered a branch of the armed forces, – not a standalone functional

service of the armed forces as in Germany.³⁴ The Commander of Cyber Command reports directly to the CHoD (known in Estonia as the Commander of the Defence Forces).

Cyber Command consists of five sub-units: the Support and Signal Battalion (SSB), the Headquarters and Support Company, the ICT Technology Centre, the Strategic Communications Centre, and the Cyber and Information Operations Centre.³⁵ In addition, the Headquarters of the Estonian Defence Forces has a Control and Communication Systems Department (also known as the Signals Department, J6) that coordinates and executes oversight in cyber defence issues of the Estonian Defence Forces, and a Strategic Communication Department that organises strategic communications of the Estonian Defence Forces and issues guidelines for the implementation of strategic communication activities.³⁶ The Strategic Communications Centre of Cyber Command implements these activities at the operational level.³⁷

Cyber Command has leadership and headquarters/staff components that directs the planning of cyber and reconnaissance activities while planning and directing military operations.³⁸ The headquarters component coordinates cyber defence capabilities and cooperates with other actors within the defence organisation, as well as those in the Estonian public and private

²⁹ "National Defence Act," paragraph 13, 1.

³⁰ "National Defence Act," paragraph 5, 1.

³¹ Ministry of Defence, "The National Defence Development Plan 2017-2026."

³² Erki Kodar (presentation at the NATO cyber symposium NIAS'17, Mons, Belgium, October 17-19, 2017), <https://www.youtube.com/watch?v=PKC-nWRfez4> (accessed November 5, 2018).

³³ "Luik: Eesti on vajadusel valmis andma oma kübervõimed NATO käsutusse" [Luik: If requested Estonia is ready to give its cyber capabilities to NATO], *Eesti Rahvusringhääling (ERR)*, October 4, 2018, <https://www.err.ee/866519/luik-eesti-on-vajadusel-valmis-andma-oma-kubervoimed-nato-kasutusse> (accessed November 5, 2018).

³⁴ A branch is part of military service, and it holds special armament and battle equipment. Other branches of the Estonian defence Forces are for example: communications, electronic intelligence, infantry, pioneer, anti-air warfare, and artillery. In addition to planning and executing cyberspace operations, Cyber Command has service-like responsibilities to build forces through education, training, exercises for conscripts and reserve forces. Interviews conducted with Estonian experts in Tallinn, December, 2017.

³⁵ Headquarters of the Estonian Defence Forces, "Küberväejuhatuse põhimäärus," [Statute of Cyber Command], the CHoD degree no 149, July 9, 2018, <http://www.mil.ee/UserFiles/sisu/kaitsevagi/organisatsioon/kv%20oigusaktid/KVPS%20p%C3%B5him%C3%A4%C3%A4rus.pdf> (accessed November 7, 2018).

³⁶ Headquarters of the Estonian Defence Forces, "Headquarters."

³⁷ "Kaitseväge peastaabi põhimäärus" [Statute of Cyber Command], Headquarters of the Estonian Defence Forces, "Headquarters," <http://www.mil.ee/en/defence-forces/Headquarters-of-the-Estonian-Defence-Forces> (accessed November 7, 2018).

³⁸ "Küberväejuhatuse põhimäärus" [Statute of Cyber Command].

sectors and international partners.³⁹ Elevating the function of planning and executing cyberspace operations to a position directly under the CHoD allows better coordination with military operations while creating a lean cyber command structure. The creation of a command would justify allocating greater financial and human resources to cyber defence.⁴⁰

Elevating the function of planning and executing cyberspace operations to a position directly under the CHoD allows better coordination with military operations while creating a lean cyber command structure

Functions

The key functions of Cyber Command are:

- 1) organising command support, cyber defence, and the development and functioning of ICT for the country's whole defence organisation; and
- 2) organising information and cyber operations.⁴¹

In order to fulfil these functions, the command directs and coordinates the development of cyber capabilities and command support capabilities, and organises the preparation and formation of wartime and reserve units, the training of conscripts for cyber defence and the work environment for the Headquarters of the Estonian Defence Forces. It also supports

and ensures strategic communications for the armed forces.⁴²

For its part, the Cyber and Information Operations Centre plans and coordinates cyber and information operations while defending the whole defence organisation against cyber threats. It includes the following sub-units: the Cyber and Information Operations Direction Centre, the Planning Team, the CIRC, the Cyber Operations Team, and the Cyber Range.⁴³ The Cyber Range, located in SSB in Tallinn, was founded in 2011. In 2014 it was transformed into a NATO Cyber Range and in 2016 and in 2018, the Alliance invested into its further development.⁴⁴

The NATO Cyber Range has been used for multinational technical cyber defence exercises such as NATO's Cyber Coalition and NATO CCD COE's Locked Shields.

Situational Awareness

Cyber Command will provide cyber situational awareness for the armed forces, which in the future will be linked to a national-level security threat situational picture.⁴⁵ At the national-level, situational awareness and threat analysis supplied by the relevant state authorities, including the armed forces, will be consolidated in the Situation Centre of the Prime Minister's

³⁹ "Kübertõrjehutuse põhimäärus" [Statute of Cyber Command]. At the national level the principal operational-level coordinator is the Information System Authority under the Ministry of Economic Affairs and Communications, which organises the protection of critical national information infrastructure, provides ICT services for state and municipal agencies, and includes both national and government CERTs. Minister of Economic Affairs and Communication, "Riigi Infosüsteemi Ameti põhimäärus" [Statute of the Information System Authority], regulation no 28, April 25, 2011, <https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv> (accessed November 7, 2018).

⁴⁰ The Estonian Defence Forces recognise that greater investment in people, equipment, and capabilities in the area of cyber defence are required in the near future. "ICDS seminar with General Riho Terras and Major-General Martin Herem," International Centre for Defence and Security, November 5, 2018, Tallinn.

⁴¹ Government, "Kaitseväge põhimäärus" [Statute of the Defence Forces], regulation no 45, Jun 21, 2018, <https://www.riigiteataja.ee/akt/128062018008> (accessed November 7, 2018).

⁴² All sub-units of Cyber Command prepare wartime and reserve units, including by organising conscript training in the area of cyber defence. "Kübertõrjehutuse põhimäärus," [Statute of Cyber Command].

⁴³ At the same time, there are overlapping functions between sub-units of Cyber Command – the ICT Technology Centre also encompasses several military CIRC functions such as monitoring, incident prevention and response, etc. "Kübertõrjehutuse põhimäärus" [Statute of Cyber Command].

⁴⁴ For example, in 2018 the Alliance allocated €3.9 million for further development of the cyber range. Ministry of Finance, "2018. aasta riigieelarve seaduse seletuskiri" [Explanatory note for state budget of 2018], <https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigieelarve-ja-majandus/riigieelarve-ja-majandusulevaated> (accessed October 6, 2018). Ministry of Defence, "NATO Investing in the Development of Estonian Cyber Range," June 14, 2016, <http://www.kaitseministeerium.ee/en/news/nato-investing-development-estonian-cyber-range> (accessed October 5, 2018).

⁴⁵ Information System Authority, *Annual Cyber Security Assessment 2018*, page 32, <https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf> (accessed November 5, 2018).

Office.⁴⁶ Interestingly, while the SSB's former responsibilities included conducting defence-oriented electronic warfare research and development projects, it does not retain these tasks in the new organisational structure. Moreover, while the staff component of Cyber Command directs the planning of reconnaissance activities of the command it does not possess ISR capability. Accordingly, Cyber Command will receive situational awareness from the Military Intelligence Centre of the Estonian Defence Forces, falling directly under the CHoD.

The Military Intelligence Centre provides early warning for country's military defence, organises security and intelligence activities and provides threat assessment and situational awareness for the whole defence organisation.⁴⁷ In addition, the Estonian Foreign Intelligence Service (under the jurisdiction of the Ministry of Defence) collects and processes information about foreign states by electronic means; it also provides professional assistance in the area of military intelligence to the whole defence organisation.⁴⁸

Assistance to the Civilian Authorities

Cyber Command is not expected to play a role in assisting civilian authorities in case of serious cyber attacks against the nation or its critical infrastructure.⁴⁹ The Information System Authority under the Ministry of Economic Affairs and Communications is responsible at all times for coordinating the provision of cyber security and the prevention and resolution of cyber incidents. This includes coordinating national responses to large-scale cyber incidents.⁵⁰ In addition, Estonia possesses a

Cyber Defence Unit of the Estonian Defence League (CDU), which can be deployed both in normal conditions as well as in case of emergency and crisis to assist civilian authorities in cyber security.⁵¹ The CDU must attain greater responsibilities in ensuring military cyber defence in wartime, including

The CDU must attain greater responsibilities in ensuring military cyber defence in wartime, including assuming some responsibility for forming cyber reserve forces

assuming some responsibility for forming cyber reserve forces, which currently is the role of Cyber Command. Even though the Estonian Defence League has a statutory obligation to prepare capabilities for military defence and participate in ensuring cyber security under the direction of relevant authorities, it has no statutory cyber defence role in wartime.⁵²

⁴⁶ In 2017, €7.1 million was allocated to the development of the Situation Centre. Ministry of Finance, "2017. aasta riigieelarve seaduse seletuskiri" [Explanatory note for state budget of 2017], <https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigieelarve-ja-majandus/riigieelarve-ja-majandusulevaated> (accessed October 6, 2018).

⁴⁷ "Kaitseväge põhimäärus" [Statute of the Defence Forces].

⁴⁸ Parliament, "Security Authorities Act" passed on December 12, 2000, <https://www.riigiteataja.ee/en/eli/521062017015/consolide> (accessed November 7, 2018).

⁴⁹ Interviews conducted with Estonian experts in Tallinn, December, 2017.

⁵⁰ In case of an immediate serious cyber threat or serious cyber incident provided that certain condition stipulated by law are met the Information System Authority is authorised to access a network and information system or restrict the use of or access to the system. Parliament, "Cybersecurity Act" paragraphs 16 and 17, <https://www.riigiteataja.ee/en/eli/523052018003/consolide> (accessed November 7, 2018).

⁵¹ The Estonian Defence League, as part of the Estonian Defence Forces, is a voluntary militarily organised national defence organisation; the CDU is one of its structural units. The CDU can be deployed under the guidance of the Ministry of Defence (or other authorities falling under the Ministry of Defence area of governance) or the Information System Authority upon the decision of the Commander of the Estonian Defence League. Upon deployment, the CDU's mandate is to ensure the functioning of (and mitigate cyber threats to) ICT infrastructure that supports essential services and state functions, including in the private sector. See Kadri Kaska, Anna-Maria Osula, Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis*, (Tallinn: NATO CCD COE, 2013), https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (accessed October 16, 2018). Government, "Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel" [Requirements and order of engaging the Defence League in ensuring cyber security], regulation no 108, July 3, 2014, <https://www.riigiteataja.ee/akt/110072014003> (accessed November 7, 2018). Estonian Defence League, <http://www.kaitseliit.ee/en/edl> (accessed November 7, 2018).

⁵² The majority of CDU members are civilian professionals and thus cannot presently be assigned to military operations unless they are also part of the reserve forces. Parliament, "The Estonian Defence League Act," passed on February 28, 2013, <https://www.riigiteataja.ee/en/eli/530042018001/consolide> (accessed November 5, 2018).

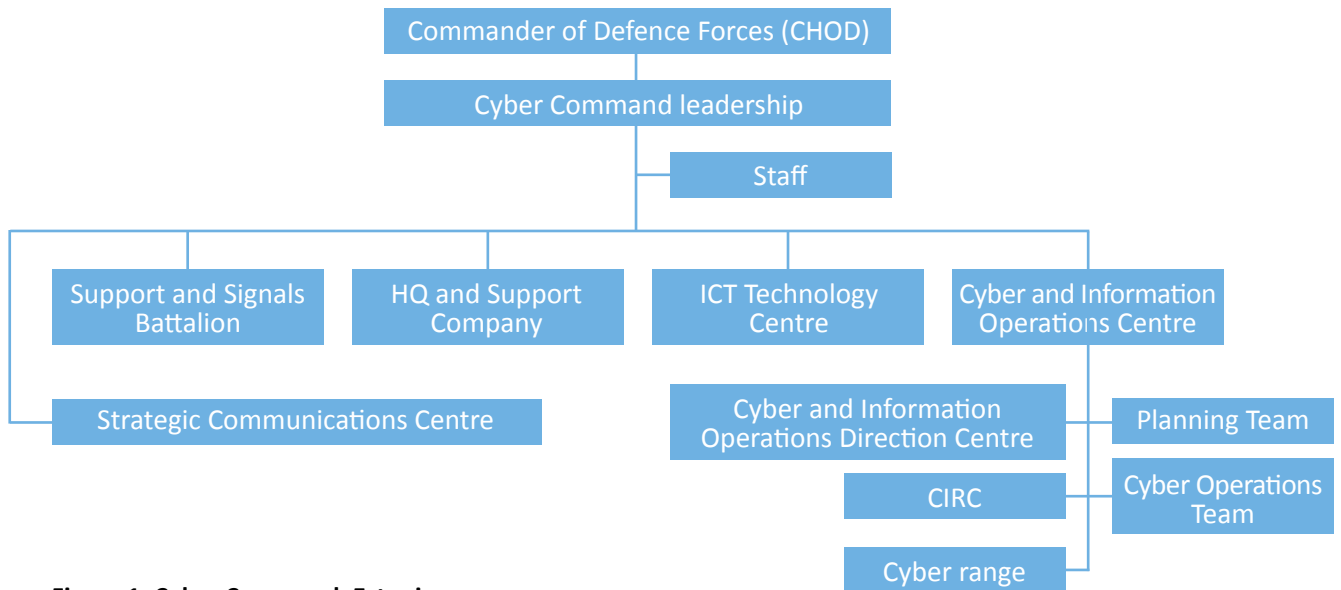


Figure 1. Cyber Command, Estonia

2.2. FINLAND: CYBER DIVISION OF THE C5 AGENCY

Strategic Guidelines

According to Finland's cyber security strategy of 2013, the Finnish Defence Forces were to create a comprehensive cyber defence capability encompassing intelligence, cyber defence and cyber attack capabilities in order to fulfil their statutory tasks.⁵³ In line with the 2014 guidelines of the Finnish Government Security Committee, the Ministry of Defence is responsible for safeguarding the Finnish Defence Forces' networks and operations, defending the nation against grave cyber attacks, developing intelligence, defence and offensive cyberspace capabilities, including capabilities required for deployment in international missions.⁵⁴ Pursuant to the 2017

Finnish Government Defence report to Parliament, the defence forces will establish the capabilities for providing cyber situational awareness, planning and implementing cyberspace operations, and protecting and monitoring their own systems in the cyber domain.⁵⁵ The Finnish Defence Forces' Cyber Defence Concept was issued in 2016.⁵⁶

Political Authorisation of International Deployments

The decision to participate in international crisis management is made on a case-by-case basis by the president on the basis of a proposal put forward by the government, which must previously consult Foreign Affairs Committee (or if an operation is not based on a UN Security Council mandate or is a particularly demanding military challenge, Parliament as a whole).⁵⁷ This regulation also pertains to the deployment of offensive cyberspace capabilities as part of international deployments.

⁵³ In the original Finnish version of the Cyber Security Strategy the cyberattack capability is referred to obliquely as vaikuttamine kybertoimintaympäristössä (literally "the ability to influence the cyber environment"). However, the official translation of the strategy in English uses the term "cyber attack capability". Secretariat of the Security Committee, *Finland's Cyber Security Strategy*, (Helsinki: January 21, 2013), p. 8, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (accessed November 7, 2018); According to The Military Balance 2017, Finland is developing military cyber defence capacity that encompasses intelligence and cyber attack capabilities. James Hackett, ed. *The Military Balance: The Annual Assessment of Global Military Capabilities and Defence Economics* (London: Routledge & The International Institute for Strategic Studies, 2017), p. 108, 163.

⁵⁴ The Security Committee, "Ministeriöiden kyberturvallisuustehtävät" [Cyber Security Tasks of Ministries]. February 10, 2014, <https://turvallisuuskomitea.fi/ministerioiden-kyberturvallisuustehtavat/> (accessed November 7, 2018).

⁵⁵ Prime Minister's Office, *Government's Defence Report*, (Helsinki: February 6, 2017), https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf (accessed November 7, 2018).

⁵⁶ This document is not publicly available. Interviews conducted with Finnish experts, December, 2017.

⁵⁷ Ministry of Defence, "Act of Military Crisis Management," March 31, 2006, <http://www.finlex.fi/en/laki/kaannokset/2006/en20060211.pdf> (accessed November 7, 2018).

Organisation

A military structure comparable to a cyber command in the broader meaning is the Cyber Defence Division, founded in January 2015 within the Finnish Defence Forces C5 Agency (hereinafter C5 Agency, *Puolustusvoimien johtamisjärjestelmäkeskus* [lit. Defence Forces Command and Control Centre]). The C5 Agency is a subordinate agency of the Finnish Defence Forces Headquarters that combines J6 functions of protecting the CIS as well as command, control, communications, computers, cyber (C5) functions.⁵⁸ In addition to a headquarters/staff component, it has three departments in 18 locations. The Finnish Defence Forces Headquarters has additionally a Management System Department (*Pääesikunnan johtamisjärjestelmä-osasto*) that is responsible for operational planning of cyber defence aspects.⁵⁹ In addition to these organisations, the traditional military services (army, air force, navy) have integral cyber defence capabilities.

The overall number of C5 Agency employees is 400; a majority are civilian personnel. The Cyber Division, located in Jyväskylä, protects the armed forces' data networks and services, develops cyber defence capabilities and maintains national cyber defence situational awareness. In 2015 Cyber Division had a workforce composed of less than 100 military and civilian personnel; however, in 2016 the Finnish national broadcaster reported that the size of the division will increase.⁶⁰ Similarly, *Fifth Domain* reported that the C5 Agency needs to fill at least 200 high-end ICT

and cybersecurity specialist positions by 2024; financing of the agency will be increased as a result.⁶¹

Functions

The Finnish experts interviewed concurred that Finland does not need a cyber command. One expert advocates the integration of cyber units into traditional military services, rhetorically asking "whom would it [a cyber command] command," referring to the small number of cyber specialists.⁶² The responsibility for protecting operational ICT networks belong to the departments of the C5 Agency – the IT Services Division maintains and develops operational information systems while integrating ICT; while several CIS support divisions maintain security technology, provide operational IT support, and assist in ICT training activities.⁶³

The Finnish experts interviewed concurred that Finland does not need a cyber command

According to the above-mentioned 2017 government report to Parliament, the Finnish Defence Forces have developed cyber defence capabilities that allow the protection of military functions.⁶⁴ According to the CHoD, in 2014 the Cyber Division of C5 Agency was primarily responsible for cyber defence functions within the defence forces, however, it also developed offensive cyberspace capabilities that need to be refined.⁶⁵

The specific tasks of the Cyber Division regarding its two key functions – cyber defence and cyber situational awareness – are not made

⁵⁸ For the sake of clarity, as mentioned above, the term "defence forces headquarters" is used in this report for all countries. The official English translation at the Finnish Armed Forces website for Pääesikunta is however the "Defence Command." The Defence Command is the joint command headquarters of the commander of the Finnish Defence Forces. See The Finnish Defence Forces, "Defence Command Finland," <http://puolustusvoimat.fi/en/about-us/defence-command> (accessed November 7, 2018).

⁵⁹ The Finnish Defence Forces, "Pääesikunnan johtamisjärjestelmäosasto" [The Finnish Defence Forces Headquarters Management System Department], <http://puolustusvoimat.fi/tietoa-meista/paaesikunta/johtamisjarjestelmaosasto> (accessed November 7, 2018).

⁶⁰ "Puolustusvoimat perustaa uuden kyberyksikön – hybridisotiin varaudutaan vahvistamalla verkkopuolustusta" [Defence Forces establish a new cyber unit – network defence will be fostered in order to prepare for hybrid wars], *YLE*, September 25, 2014, <https://yle.fi/uutiset/3-7491555> (accessed November 7, 2018). "Puolustusvoimat on moninkertaistamassa kyberyksikkönsä koon – "Suorituskykyämme testataan joka päivä," [Defence Forces multiplies the size of a cyber unit – "Our capabilities are tested daily," *YLE*, May 30, 2016, <https://yle.fi/uutiset/3-8906483> (accessed November 7, 2018).

⁶¹ Gerard O'Dwyer, "The Threat to Finland's Cyberdefense? Private-sector Salaries," *Fifth Domain*, <https://www.fifthdomain.com/international/2018/02/05/the-threat-to-finlands-cyberdefense-private-sector-salaries/> (accessed November 7, 2018).

⁶² Instead, in this expert's view, the armed forces should develop cyber units that are regularly trained at realistic exercises and equipped with state-of-the-art cyber capabilities. Interviews conducted with Finnish experts, December, 2017.

⁶³ The Finnish Defence Forces, "Finnish Defence Forces C5 Agency," <http://puolustusvoimat.fi/en/about-us/c5-agency> (accessed November 7, 2018).

⁶⁴ Parliament, Defence Committee, "Valiokunnan mietintö" [Committee's Consideration] PuVM 4/2017 vp – VNS 3/2017 vp. https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/PuVM_4+2017.pdf (accessed November 7, 2018).

⁶⁵ "Puolustusvoimat perustaa uuden Kyberyksikön."

publicly available. However, it is known that the Division supports the Operations Division of the Defence Forces Headquarters in integrating cyber effects into the planning and execution of military operations. Furthermore, Cyber Division is also responsible for organising cyber defence education, training, and exercises for the whole of the armed forces.⁶⁶ Training of conscripts in the area of cyber defence takes place in the C5 Agency, as well as in other military facilities.⁶⁷ Position descriptions of cyber specialists and the concomitant education, training and exercise requirements are being developed along similar lines to the analogous initiatives in Germany and the Netherlands.⁶⁸

Finland is likely to experience the same challenges in recruitment of competent staff faced by other armed forces

Concerning the need of developing voluntary military cyber forces that are capable of supporting active duty cyber operators, the Finnish experts interviewed believe that the reserve system facilitates the contribution of civilian professional cyber expertise to the military, and the Finnish cyber conscription system, active since 2015, provides a sufficient number and quality of cyber personnel for the armed forces.⁶⁹ However, since the Cyber Division is expected to grow in size and because the annual number of conscripts in the cyber defence area is very small, Finland is likely to experience the same challenges in recruitment of competent staff faced by other armed forces.

⁶⁶ In 2016, the Defence Forces created an annual cyber defence exercise combining the technical and operational levels. The purpose is to train command and control, situational awareness, and cyber defence specialists while evaluating their readiness. There is also a technical level cyber exercise that allows the capabilities of individual specialists to be further tested; moreover, each military service conducts annual technical level cyber defence exercises. Interviews conducted with Finnish experts, December, 2017.

⁶⁷ After receiving 8-week basic training, conscripts who claim to possess basic skills in programming, network technology, software development, or related fields must pass a test; successful candidates then receive specialised training in specific areas such as penetration testing, communications, computer programming, building and testing the security of ICT systems, and blue/red team activities. Interviews conducted with Finnish experts, December, 2017.

⁶⁸ Interviews conducted with Finnish experts, December, 2017.

⁶⁹ Interviews conducted with Finnish experts, December, 2017.

Situational awareness

The Finnish Defence Intelligence Agency (*Puolustusvoimien tiedustelulaitos*, PVTIEDL) is the signals, geospatial and imagery intelligence agency responsible for collecting cyber intelligence for the military. It is subordinate to the Finnish Defence Forces Headquarters' Intelligence Division which coordinates military intelligence information gathering and processing, while also providing an early warning capability.⁷⁰ At the time of writing, the Finnish Parliament is considering a package of draft intelligence legislation. According to these regulations, the PVTIEDL will be granted the authority to conduct internet and telecommunications surveillance to carry out its statutory responsibilities both in and outside Finnish territory.⁷¹ The Finnish Security Intelligence Service (*Suojelupoliisi*, SUPO), subordinated to the Ministry of the Interior, collects information on telecommunication networks and identifies and responds to cyber threats posed by foreign states. The pending legislative proposal will grant it greater authority to carry out civilian intelligence collection in Finland and abroad.⁷²

While there is no plan to give the Cyber Defence Division permission to collect digital intelligence in Finland or abroad, collecting digital intelligence is nevertheless necessary to compile a complete cyber situational picture. Thus, in order to carry out one of its main responsibilities – to maintain situational awareness – the Cyber Defence Division must cooperate with the PVTIEDL and with the SUPO.

Finally, like its Dutch and Norwegian counterparts but in contrast to its German equivalent, the C5 Agency's functions do not include electronic warfare and information operations.

⁷⁰ The Finnish Defence Forces, "Defence Command Intelligence Division," <https://puolustusvoimat.fi/en/intelligence-division> (accessed November 10, 2018).

⁷¹ Ministry of Defence, "Kysymyksiä ja vastauksia toimittajille sotilastiedustelulainsäädäntöön liittyen" [Questions and Answers to editors about the military intelligence legislation], https://www.defmin.fi/ajankohtaista/luonnos_hallituksen_esitykseksi_laiksi_sotilastiedustelutoiminnasta_ja_eraiksi_siihen_liittyviksi_laeiksi (accessed November 10, 2018).

⁷² Ministry of the Interior, "Civilian intelligence legislation would improve Finland's national security," press release 9/2018, January 25, 2018, https://intermin.fi/en/artikkeli/-/asset_publisher/siviilitiedustelulaki-parantaisi-suomen_kansallista-turvallisuutta (accessed November 10, 2018).

Assistance to the Civil Authorities

The Finnish Defence Forces do not have a statutory responsibility to support the civilian authorities in case of a “cyber emergency” or a serious cyber incident that impairs the essential functions of society or the operation of critical national infrastructure. In Finland,

whole-of-society and whole-of government approaches (which are coordinated centrally by the relevant civilian authorities) have been well developed and implemented, thus explaining why the armed forces have not needed to develop such capabilities by themselves.

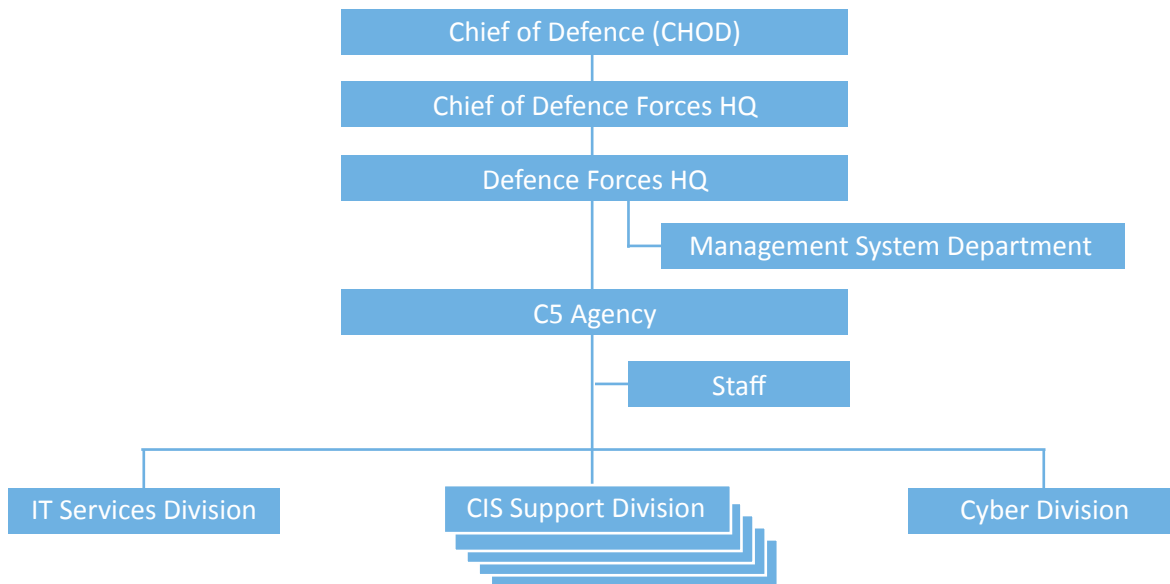


Figure 2. Cyber Division of C5 Agency, Finland (simplified model)

2.3. GERMANY: CYBER AND INFORMATION DOMAIN SERVICE

Strategic Guidelines

Strategic guidelines pertaining to the role of the German military in cyber security are set out in the Cyber Security Strategy (*Cyber-Sicherheitsstrategie für Deutschland*) issued under the lead of the Federal Ministry of the Interior in 2016, and in the Defence White Paper (*Weissbuch*) produced that year by the Federal Ministry of Defence.⁷³ According to these documents, the German Armed Forces (Bundeswehr) are responsible for ensuring the cyber security of military networks and systems, defending against hybrid threats, and protecting international crisis management missions against threats from the cyber and information domain.⁷⁴

The White Paper prescribes that the Bundeswehr must “deliver effects” in cyber and information domain, however, neither strategic document explicitly refers to the development of offensive cyberspace capabilities.⁷⁵ In the cyber and information domain the Bundeswehr must foster resiliency and supply chain security, support whole-of-society cooperation and ensure military defence aspects of a whole-of-government approach to cyber security, consolidate military ICT capabilities and functions, and develop innovative workforce recruitment strategies in ICT and cyber defence.⁷⁶ The documents also note that the Bundeswehr will develop its cyberspace capabilities further and contribute to maintaining national-level situational awareness in the cyber and information domain.⁷⁷ In addition to these strategic guidelines, the Federal Ministry of Defence has adopted guidelines related to the development of ICT and of the cyber defence of the armed forces that are not publicly available;

⁷³ Federal Ministry of the Interior, *Cyber-Sicherheitsstrategie für Deutschland* 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (accessed November 10, 2018); Federal Ministry of Defence, *White Paper on German Security Policy and the Future of the Bundeswehr*, (Berlin: June 2016).

⁷⁴ Federal Ministry of Defence, *White Paper*, pp. 91-92.

⁷⁵ Federal Ministry of Defence, *White Paper*, p. 102.

⁷⁶ Federal Ministry of Defence, *White Paper*, p. 93.

⁷⁷ Federal Ministry of Defence, *White Paper*, p. 93.

in the future, Cyber Defence Doctrine along with other relevant policies will be developed.⁷⁸

Political Authorisation of International Deployments

Pursuant to the German constitution and the Parliamentary Participation Act of 18 March 2005, the German government must obtain prior consent of the Parliament (Bundestag) in order to deploy military forces in international military operations, including cyberspace operations. In emergency situations, consent of the Parliament may be given retroactively.⁷⁹

The Bundeswehr must support whole-of-society cooperation and ensure military defence aspects of a whole-of-government approach to cyber security

Organisation

The German military perceives the cyberspace and electromagnetic spectrum as forming part of the broader information environment.⁸⁰ In keeping with this holistic view, the capabilities of the armed forces related to information, cyber and electronic warfare were integrated in April 2017 into a new functional service of the armed forces, which is called the Cyber and Information Domain Service (*Organisationsbereich Cyber- und Informationsraum*, CIR).⁸¹ The new service of Bundeswehr has a headquarters/

staff component (*das Kommando Cyber- und Informationsraum*, KdoCIR) located in Bonn.

As part of Bundeswehr CIR is sub-ordinated to the Federal Ministry of Defence; it receives strategic guidance through the Directorate-General Cyber/IT and the Directorate-General Strategy and Operations.⁸² The Directorate-General Cyber/IT, which is led by a Chief Information Officer, was founded only in October 2016. It is responsible for the protection of the Bundeswehr's networks and systems, it plans and implements defence aspects of whole-of-government cyber security, as well as plans and coordinates national and international cyber and IT activities within the remit of the Federal Ministry of Defence. It has two sub-divisions: an IT Governance Division in Berlin and an IT Services/Information Security Division in Bonn. The Directorate-General Strategy and Operations is responsible for planning and execution of military operations; in these matters it is accountable to the Executive Group of the Ministry of Defence.⁸³ At this stage it seems that the division of responsibilities regarding cyber defence between these two Directorates-General has not yet been fully established.

The majority of CIR's workforce was transferred from other services and all sub-units of CIR have remained in their former locations. In July 2017 the initial operational capability was attained – consisting of approximately 13,500 military and civilian positions; full operational capability is expected to be reached in 2021, by which time it will have a staff of about 14,500 (an increase of only 1,000).⁸⁴

CIR is commanded by a Chief (*Inspekteur*, InspCIR) at the three-star rank of lieutenant general who is also a Commander of KdoCIR.⁸⁵ The Deputy Chief supports InspCIR in fulfilling his or her tasks with respect to the entire military cyber service, while the Chief of Staff

⁷⁸ Interviews conducted with German experts, January, 2018.

⁷⁹ In the case secrecy is required for the success of an operation, the German government can decide on the deployment of armed forces upon informing specific members of the Bundestag's Defence Committee. An emergency situation is defined as "an event of imminent danger that allows no scope for delay," Katja S. Ziegler, "The Model of a 'Parliamentary Army' Under the German Constitution," Memorandum, Minutes of Evidence, Select Committee on Constitution, House of Lords, Parliament, <https://publications.parliament.uk/pa/ld200506/ldselect/ldconst/236/5120707.htm> (accessed November 10, 2018); Federal Constitutional Court, "On the Scope of the Requirement of Parliamentary Approval for Deployments of the Armed Forces in Cases of Imminent Danger," press release no. 71/2015, September 23, 2015, <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2015/bvg15-071.html> (accessed November 10, 2018); Isabel Skierka, "Bundeswehr: Cyber Security, the German way," *Digital Frontiers*, October 20, 2016, <https://www.orfonline.org/expert-speak/bundeswehr-cyber-security-the-german-way/> (accessed November 10, 2018).

⁸⁰ In this paper the terms "German Armed Forces," "Bundeswehr," and "German military" are used synonymously.

⁸¹ Ursula von der Leyen, the German Defence Minister, announced the intention to create CIR in September 2015, and the process of its establishment began in April 2016. Two other functional services are Medical Service and Joint Support Service.

⁸² Interviews conducted with German experts, January, 2018.

⁸³ Federal Ministry of Defence, "The Directorates General," <https://www.bmvg.de/en/organisation/the-directorates-general> (accessed November 10, 2018)

⁸⁴ Federal Ministry of Defence, "FAQ: Cyber-Abwehr," <https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr> (accessed November 10, 2018)

⁸⁵ CIR is considered to be at the same level with other services of the Bundeswehr (army, air force, navy, medical service, and joint service) which are also commanded by three-star generals or equivalent.

provides support in supervising command, operations, and planning functions of KdoCIR. KdoCIR serves as the single national and international point of contact for Bundeswehr Information Technology (IT) and cyber security matters. As of April 2018, it had 540 positions.⁸⁶

Functions

CIR integrates three former military organisations under a single command:

- 1) the Bundeswehr Information Technology Command (*das Kommando Informationstechnik der Bundeswehr*);
- 2) the Strategic Reconnaissance Command (*das Kommando Strategische Aufklärung*)
- 3) the Bundeswehr Geoinformation Centre (*das Zentrum für Geoinformationswesen der Bundeswehr*).

The streamlining and consolidation of formerly fragmented capabilities was performed in order to accelerate decision-making processes, shorten the time required for the adoption of new technology, and accomplish cyber defence tasks

According to the German officials interviewed the streamlining and consolidation of formerly fragmented capabilities was performed in order to accelerate decision-making processes, shorten the time required for the adoption of new technology, and accomplish cyber defence tasks as stipulated in national strategic guidelines.⁸⁷ The following capabilities were centralised: IT services/CIS support, military reconnaissance, signal intelligence, electronic warfare, geoinformation, and operational communications (including strategic communications and information operations activities).

The Information Technology Command includes a headquarters/staff component, six battalions, a school, a cyber security centre, an IT-operations centre, and the German component of the 1st NATO Signal Battalion. The 24/7 cyber

security centre was launched in April 2017 in Euskirchen (with 40 newly created positions) and it includes the Bundeswehr CERT (CERTBw), which is responsible for cyber incidence response in Bundeswehr networks and systems, including deployed networks in international crisis management missions. Other field offices of the Information Technology Command remain in their former locations in Reinbach and Pöcking; the staff component is in Bonn. In April 2019 a Software Competence Centre of the Information Technology Command will be opened.⁸⁸

The German Armed Forces Operations Command and KdoCIR are jointly responsible for the military-strategic and operational-level planning and execution of cyberspace operations. However, the specific command responsibilities will be decided on a case-by-case basis, which may cause a lack of clarity in roles and responsibilities while extending the time cycles of planning and operations.

In a similar way to the Finnish and Dutch cases, KdoCIR will develop career paths for military cyber personnel in cooperation with the personnel management authorities of the Bundeswehr. Furthermore, working together with the National Defence College and other Bundeswehr education and training institutions, improvements will be made in the training programmes of military operational planners to improve their cyber defence expertise.⁸⁹

Situational Awareness

In contrast to the Netherlands Defence Cyber Command, which (as explained below) routinely shares information with the national foreign intelligence agency, the ISR, defensive,

⁸⁶ Ludwig Leinhos, "Planung und Umsetzung der Abteilung Cyber/IT (CIT) und des OrgBer Cyber- und Informationsraum (CIR)," [Planning and Implementation of the Cyber/IT (CIT) Department and the OrgBer Cyber and Information Domain (CIR)], https://www.afcea.de/fileadmin/user_upload/News/Dokumente/Vortrag_KO_IT-Tagung_Leinhos_LtrAufbStab_CyberInfoR.pdf (accessed November 10, 2018).

⁸⁷ Interviews conducted with German experts, January, 2018.

⁸⁸ Stefan Königsmark, "Wachstum steuern – der Aufwuchs aus organisatorischer Sicht," *Sonderausgabe - Cyber- und Informationsraum, Europäische Sicherheit & Technik*, Mittler Verlag GmbH, pp. 37-39.

⁸⁹ The key partners in the area of education and training are the Bundeswehr University in Munich, which provides academic education for all German military services, and the Cyber Innovation Hub in Berlin, which brings together active officers, reservists, and civilian professionals in order to accelerate the digitisation of the German armed forces. From 2018 the Bundeswehr University will offer a masters' programme in cyber security. In order to attract talented students, scholarships will be offered. See Heiner Kiesel, "Bundeswehr Cybersecurity Center Trains Elite Counterhackers," April 1, 2018, *Deutsche Welle*, <http://www.dw.com/en/bundeswehr-cybersecurity-center-trains-elite-counterhackers/a-43210036> (accessed November 10, 2018).

and offensive cyberspace operations of the Bundeswehr are kept separate from those of national intelligence services. Legal and administrative cooperation frameworks between intelligence services and the armed forces have not been concluded since such cooperation remains politically sensitive. German intelligence services include the Federal Intelligence Service (*Bundesnachrichtendienst*, BND) and the domestic intelligence agency, the Federal Office for the Protection of the

communications, intelligence, space, army, Counter-Improvised Explosive Devices, etc.⁹³ The centre will share information with competent public authorities and provide input to the National Centre for Cyber Defence (*Nationales Cyber-Abwehrzentrum*, NCAZ).⁹⁴ NCAZ combines personnel from all relevant entities (for example, KdoCIR, the Federal Police, BND and BfV) and from industry. With its forthcoming enhanced project entitled “NCAZ+,” the centre will provide 24/7 situational awareness and response to cyber incidents.⁹⁵

Legal and administrative cooperation frameworks between intelligence services and the armed forces have not been concluded since such cooperation remains politically sensitive

Constitution (*Bundesamt für Verfassungsschutz*, BfV).⁹⁰ The BfV has legal mandate to collect signal and digital information in telecommunication networks.⁹¹ Both cabinet members and senior government officials have suggested that the BfV’s mandate should be expanded to include the right to use offensive cyberspace operations in response to cyber-attacks.⁹²

As part of KdoCIR, a Situation Centre will be established, which will provide a joint cyber operational picture by integrating existing capabilities in areas such as IT/CIS, operational

The Strategic Reconnaissance Command is located in Gelsdorf. It commands and controls electronic warfare battalions, an electronic warfare analysis centre, an imagery intelligence centre, a situational analysis centre, a strategic reconnaissance school, and an operational communications centre.

In April 2018 a Cyberspace Operations Centre (which will achieve full operational capability in 2022) was launched. Its initial complement is approximately 100 positions, 80 of which were transferred from the Computer Network Operations Department of the Strategic Reconnaissance Command in Rheinbach; thus, the total increase in manpower was only 20.⁹⁶ The functions of the Cyberspace Operations Centre comprise the provision of a complete cyber operational picture for the Bundeswehr, the development of offensive cyberspace operations capabilities, as well as the provision of red teaming capability for cyber defence exercises.

⁹⁰ The German Chancellery oversees the BND, while the Ministry of the Interior is responsible for the BfV. In Germany the general public is more concerned about surveillance by domestic and foreign intelligence services than those in many other countries, due to the historical experiences with such surveillance in the Nazi era and in East Germany. In 2013, former US National Security Agency (NSA) contractor Edward Snowden leaked documents showing the scope of NSA surveillance in the country – as well as the extent of its cooperation with the BND – thereby prompting further concerns about surveillance practices by intelligence services in the country.

⁹¹ Federal Ministry of Justice and Consumer Protection, “Bundesverfassungsschutzgesetz” [The Federal Constitution Protection Law], paragraph 3, section 1 and 2, <https://www.gesetze-im-internet.de/bverfsg/3.html> (accessed November 10, 2018).

⁹² For example, the Minister of the Interior and the Head of BfV have recently argued that the agency’s legal mandate be expanded. See Andrea Shalal and Thomas Escritt, “In Cyber, Germany Needs to Counter-attack, Minister Says,” *Reuters*, July 24, 2018, <https://uk.reuters.com/article/uk-germany-espionage-cyber/in-cyber-germany-needs-to-counter-attack-minister-says-idUKKBN1KE0YG> (accessed November 10, 2018). Andrea Shalal, “German Spy Agencies Want Right to Destroy Stolen Data and ‘Hack Back’,” *Reuters*, October 5, 2017, <https://www.reuters.com/article/us-germany-cyber/german-spy-agencies-want-right-to-destroy-stolen-data-and-hack-back-idUSKBN1CA11N> (accessed November 10, 2018).

⁹³ Interviews conducted with German experts, January, 2018. Federal Ministry of Defence, “FAQ: Cyber-Abwehr,” Armin Fleischmann, “Perspektiven und Herausforderungen im zukünftigen OrgBer Cyber- und Informationsraum (CIR),” [Perspectives and Challenges in the Future OrgBer Cyber and Information Space (CIR)], https://www.afcea.de/fileadmin/user_upload/News/Dokumente/Vortrag_10_Fleischmann.pdf (accessed November 10, 2018).

⁹⁴ The National Cyber Response Centre is a subordinate agency of the Federal Ministry of the Interior that additionally reports to the Federal Office for Information Security (BSI). Federal Office for Information Security, “Cyber-Abwehrzentrum,” <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum.html> (accessed November 10, 2018).

⁹⁵ The decision on the centre’s physical location will be made in 2018, and it will become operational in 2019. Interviews conducted with German experts, January, 2018.

⁹⁶ Fleischmann, “Perspektiven und Herausforderungen.”

Assistance to the Civilian Authorities

According to the White Paper, the protection of critical national infrastructure will be carried out jointly by all state authorities and other actors as part of a whole-of-government approach under the leadership of the Federal Ministry of the Interior. For its part, the National Cybersecurity Strategy specifies that resources

of the Bundeswehr, most notably its Cyber Incident Response Teams, might be deployed in order to assist public authorities in ensuring cyber security.⁹⁷ The Bundeswehr is obliged to support other ministries as part of the principle of professional support (*Amtshilfe*), although the modalities of such assistance are subject to inter-ministerial agreements.⁹⁸

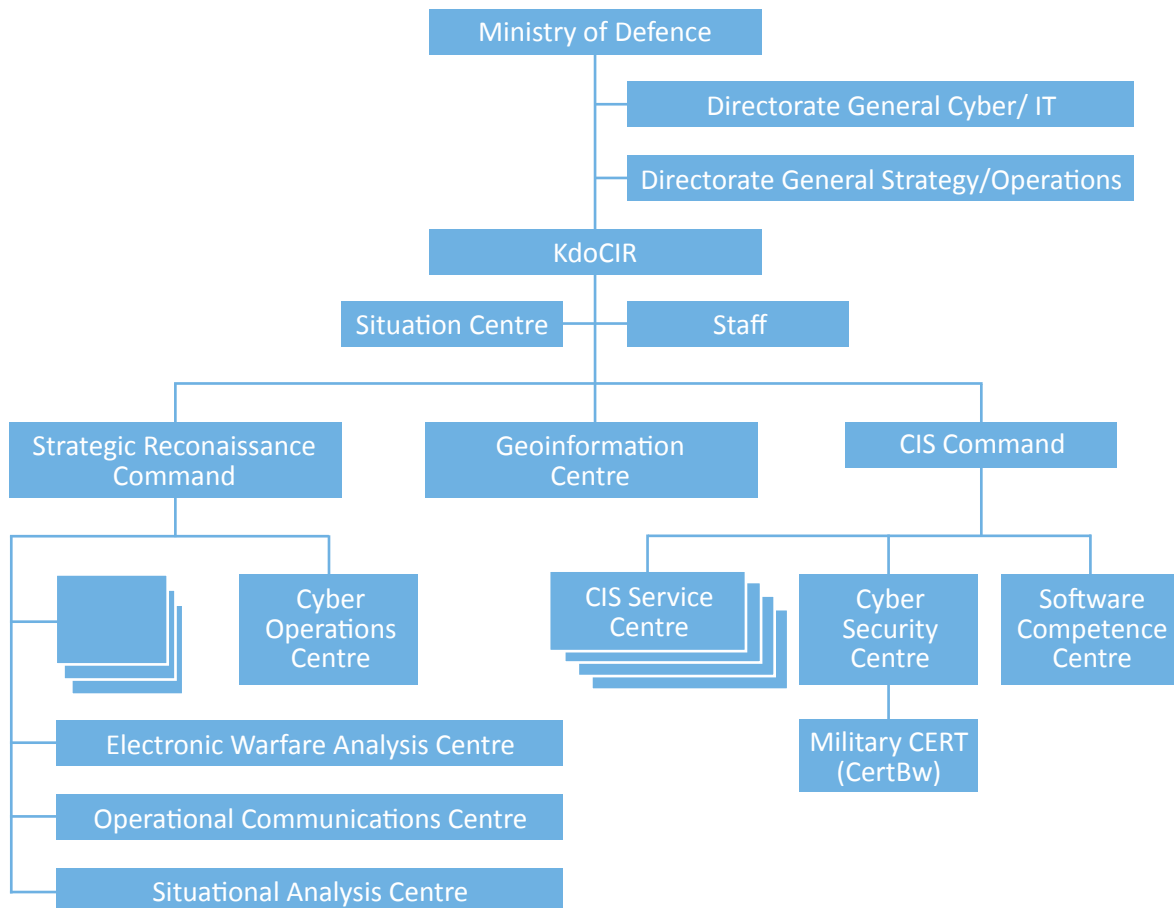


Figure 3. CIR, Germany (simplified model)

⁹⁷ Federal Ministry of the Interior, "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 29, 33.

⁹⁸ Federal Ministry of Defence, "White Paper," p. 92.

2.4. NETHERLANDS: DEFENCE CYBER COMMAND

Strategic Guidelines

The Netherlands has two strategies related to security and defence in cyberspace. In 2012 it published a Defence Cyber Strategy, updated in February 2015. The updated version of the document references a Defence Cyber Doctrine, although the latter was never adopted.⁹⁹ The latest national-level strategy, dating from 2013, is entitled “National Cyber Security Strategy 2: From Awareness to Capability.”¹⁰⁰ In May 2018, the Government of the Netherlands published a National Cyber Security Agenda and allocated €95 million for cyber security activities across several ministries, including the Ministry of Defence.¹⁰¹

The purpose of offensive cyberspace operations is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks, weapons and sensor systems

Together with the armed forces of the Netherlands (*Nederlandse krijgsmacht*) the Ministry of Defence develops and maintains defensive, offensive, and intelligence cyberspace capabilities.¹⁰² The purpose of offensive cyberspace operations is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks, weapons and sensor systems.¹⁰³ The 2015 update to the Defence Cyber Strategy sets out lines of activities (most of which were also covered in the previous version) for the armed forces:

- 1) defensive, offensive and intelligence cyberspace operations;
- 2) innovation and acquisition;
- 3) recruiting, retaining, and training personnel;
- 4) comprehensive approach and cooperation;
- 5) increasing competence and knowledge.

The updated version underlines two particular priority areas among the above activities: the acquisition process (which must become more agile to address rapid technological changes) and the development of skills and knowledge in ICT and cyber defence (which is singled out for improvement). The Dutch defence organisation recognises cyberspace as the fifth military domain of operations.¹⁰⁴ Given the necessity to prepare the armed forces to fight in this domain, there was a consensus that a special command structure be established.¹⁰⁵

Political Authorisation of International Deployments

The Netherlands has deployed a Cyber Mission Team as part of its military contribution to NATO's Enhanced Forward Presence in the three Baltic States and Poland.¹⁰⁶ It is not publicly known if this team possesses offensive cyberspace capabilities. In the Netherlands, the government decides whether to deploy armed forces in international operations, including the use of cyberspace operations by the Defence Cyber Command. The government must inform parliament prior to the deployment; in cases when this is not feasible, it must still do so as soon as possible.¹⁰⁷

⁹⁹ Ministry of Defence, *The Defence Cyber Strategy*, 2015, <https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy> (accessed November 10, 2018). At the time of writing, the document's review processes are ongoing; an updated strategy is expected to be published at the end of 2018.

¹⁰⁰ National Cyber Security Centrum, *National Cyber Security Strategy 2*, <https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html> (accessed November 10, 2018).

¹⁰¹ National Coordinator for Security and Terrorism, *National Cyber Security Agenda*, July 9, 2018, https://english.nctv.nl/binaries/CSAgenda_EN_def_web_tcm32-339827.pdf (accessed November 10, 2018).

¹⁰² Ministry of Defence, *The Defence Cyber Strategy*, page 6.

¹⁰³ Ministry of Defence, “Defence Cyber Command,” <https://english.defensie.nl/topics/cyber-security/cyber-command> (accessed November 10, 2018).

¹⁰⁴ Ministry of Defence, *The Defence Cyber Strategy*.

¹⁰⁵ Interviews conducted with a Dutch expert, January, 2018.

¹⁰⁶ Hans Folmer, “Demystifying Cyber Operations”, *Militair Rechtelijk Tijdschrift*, [Netherlands Military Law review] https://puc.overheid.nl/mrt/doc/PUC_248329_11/1/ (accessed November 10, 2018).

¹⁰⁷ Article 100 of the Dutch Constitution, enacted in 2008, states that the government must inform parliament prior to such deployment; if compelling reasons exist the government is exempt from this requirement, but must supply information to parliament as soon as possible. Government of the Netherlands, “The Constitution of the Kingdom of the Netherlands 2008,” <https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008> (accessed November 10, 2018).

Organisation

The Defence Cyber Command was created in 2014 as part of the Royal Netherlands Army and was subordinated to the CHoD only in operational matters.¹⁰⁸ On 5 July 2018, the Defence Cyber Command was elevated to a command component directly under the CHoD (Chief of Defence of the Netherlands Armed Forces). However, the Defence Cyber Command is not considered to constitute a functional military service; it incorporates cyberspace capabilities drawn from army, navy, air force, and military police.¹⁰⁹ The Commander of Defence Cyber Command is a military adviser of the CHoD on cyber issues, while the Directorate of Operations of the Ministry of Defence advises the CHoD on the deployment of cyber effects during military operations.¹¹⁰

Per the 2015 Defence Cyber Strategy, cyber aspects will be integrated into operational decision-making processes both before and after operations

The Defence Cyber Command is responsible for the development and deployment of defensive and offensive cyberspace capabilities at the operational level, while the Directorate for Policy of the Ministry of Defence is responsible for strategy and policy development.¹¹¹ Per the 2015 Defence Cyber Strategy, cyber aspects will be integrated into operational decision-making processes both before and after operations.¹¹²

Functions

The Defence Cyber Command is comprised of three departments: Operations, Technology, and the Defence Cyber Expertise Centre. In addition, it has a headquarters/staff component.¹¹³

The Department of Operations, meanwhile, consists of an intelligence component as well as Cyber Advisors who can be deployed as part of Cyberspace Operations Teams that will be established in the future. These teams will provide a full spectrum of cyberspace capabilities to operational commanders, including for example defensive and offensive cyberspace operators, operational planners, software specialists, etc. The task of the existing Advisors is to provide operational commanders with insight on issues pertaining to military cyberspace operations. Moreover, all four military services have staff officers with cyber defence expertise who coordinate the planning and execution of cyberspace operations between the service and the Defence Cyber Command.

The Department of Technology consists of cyber technicians whose role is to develop tools, tactics, techniques and procedures (TTTP) as well as skills for conducting defensive and offensive cyberspace operations.

Finally, the Defence Cyber Expertise Centre develops and provides cyber defence knowledge, education, and training for the whole defence organisation. This Centre, in cooperation with the Netherlands Organisation for Applied Scientific Research, determines the roles and required skill sets for cyber defence positions in the Dutch military. In the future the Defence Cyber Command plans to create special career paths for cyber personnel.

The Defence Cyber Command itself is currently manned on a rotational basis with officers supplied from the four military services,

¹⁰⁸ In other matters (organisation, materiel, personnel, etc.) the Defence Cyber Command was previously subordinated to the Central Staff of the Ministry of Defence. Interviews conducted with a Dutch expert, January, 2018. Ministry of Defence, "Central Staff," <https://english.defensie.nl/organisation/central-staff> (accessed November 10, 2018).

¹⁰⁹ Kadri Kaska, *National Cyber Security Organisation: the Netherlands*, (Tallinn: NATO CCC COE, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf (accessed November 10, 2018).

¹¹⁰ Interviews conducted with a Dutch expert, January, 2018. Kaska, Kadri, *National Cyber Security Organisation: the Netherlands*.

¹¹¹ Interviews conducted with a Dutch expert, January, 2018.

¹¹² Ministry of Defence, *The Defence Cyber Strategy*.

¹¹³ Maxime Zech, "Dutch Cyber Defence Centre unveiled," May 14, 2014, *NLTimes.nl*, <https://nltimes.nl/2014/05/21/dutch-cyber-defence-center-unveiled/> (accessed November 10, 2018). Matthijs Koot, "The Dutch Defense Cyber Command: A New Operational Capability," Matthijs R. Koot's notebook, <https://blog.cyberwar.nl/2014/10/the-dutch-defense-cyber-command-a-new-operational-capability-colonel-hans-folmer-2014/> (accessed November 10, 2018). Hans Folmer, "Operationeel. Defensie Cyber Commando" [Operational. Defence Cyber Command], Vereniging van Officieren van de Verbindingsdienst [Association of Signal Corps Officers], <https://vovklic.nl/intercom/2016/1/22.pdf> (accessed November 10, 2018).

although the career development paths of these officers remain the responsibility of the individual services. The number of civilian and military personnel in the Defence Cyber Command is not public.

Finally, the Defence Cyber Command has a classified cyber range.¹¹⁴ In addition, there is another cyber range that provides training and exercise environment and laboratory for research, development and testing of cyber TTPs.¹¹⁵ This cyber range is available for the use of the Dutch defence organisation as well as of its partners.¹¹⁶

Situational Awareness

The Netherlands has two intelligence services – the Defence Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*, MIVD), subordinated to the Ministry of Defence, and the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*, AIVD) under the Ministry of the Interior and Kingdom Relations. The mandates and responsibilities of the MIVD and AIVD are set out in the “Law on the Intelligence and Security Services 2002”, according to which both services have the authority to break into computer systems in foreign countries when performing their security or intelligence tasks.¹¹⁷ A new “Law on the Intelligence and Security Services 2017”, which came into effect on 1 May 2018, expands the rights of both intelligence services to collect information from telecommunication networks.¹¹⁸

The MIVD provides intelligence to the Dutch defence organisation and other relevant ministries (foreign affairs, security and justice, etc.).¹¹⁹ It intercepts telecommunications at home and abroad, conducts intelligence cyberspace operations, and contributes to the development of the Defence Cyber Command’s offensive cyberspace operations.¹²⁰ It provides cyber intelligence to operational commanders and a cyber situational picture to the Defence Cyber Command. An MIVD liaison officer is posted to the Department of Operations of the Defence Cyber Command, while personnel of the Defence Cyber Command are seconded to the Joint Signal Intelligence Cyber Unit (JSCU). Founded in June 2014 and scheduled to be reinforced in size in the next few years, the JSCU integrates the signals intelligence and cyber operations components of the MIVD and AIVD.¹²¹ The unit’s mandate is to conduct intelligence and offensive cyberspace operations for the purpose of assisting both the AIVD and MIVD in the completion of their legal tasks.¹²² Thus, this capability does not constitute an offensive cyberspace capability for the purpose of the use of force in and through cyberspace in order to conduct standalone military cyber operations or support traditional military operations.

Assistance to the Civilian Authorities

Whereas the Estonian, the German, the Finnish, and the Norwegian military cyberspace organisations (commands, service, division) all include military CIRC functions, the Netherlands is an exception. DefCERT constitutes an independent organisation subordinated to the Joint Communications & Information Services Command (JIVC) under the Defence Materiel Organisation, one of the seven organisations of the Ministry of Defence, and does not fall directly under the CHoD. DefCERT is responsible for defending the IT networks and systems of

¹¹⁴ Interviews conducted with a Dutch expert, January, 2018.

¹¹⁵ Ministry of Defence, “A Look at the Defence News 2 – 8 May,” May 10, 2016, <https://english.defensie.nl/latest/news/2016/05/10/a-look-at-the-defence-news-2-%E2%80%93-8-may> (accessed November 10, 2018).

¹¹⁶ Ministry of Defence, *The Defence Cyber Strategy*. Ministry of Defence, *The Defence Cyber Strategy*, 2012, https://ccdcoe.org/sites/default/files/strategy/NDL-Cyber_StrategyEng.pdf (accessed November 10, 2018).

¹¹⁷ This authority is set out in the article 24 of the Intelligence and Security Services Act from 2002. Review Committee on the Intelligence and Security Services, *Review Report on the Use of the Investigatory Power to Hack by the AIVD and the MIVD in 2015*, p. 10, <https://english.ctivd.nl/latest/news/2017/10/20/index> (accessed November 10, 2018).

¹¹⁸ Review Committee on the Intelligence and Security Services, “Update website CTIV,” <https://english.ctivd.nl/latest/news/2018/05/01/index> (accessed November 10, 2018). Review Committee on the Intelligence and Security Services, *Annual report CTIVD 2017*, <https://english.ctivd.nl/documents/annual-reports/2018/05/23/index> (accessed November 10, 2018).

¹¹⁹ Government of the Netherlands, *2014 Annual Report Netherlands Defence Intelligence and Security Service*, <https://www.government.nl/documents/annual-reports/2015/07/21/2014-annual-report-netherlands-defence-intelligence-and-security-service> (accessed November 10, 2018).

¹²⁰ Kadri Kaska, *National Cyber Security Organisation: the Netherlands*, p. 17. Ministry of Defence, “Netherlands Defence Intelligence and Security Service,” https://fas.org/irp/world/netherlands/mivd_brochure.pdf (accessed November 10, 2018).

¹²¹ Ministry of Defence, *The Defence Cyber Strategy*.

¹²² Review Committee on the Intelligence and Security Services, *Review Report on the Use of the Investigatory Power*, p. 10.

the Dutch defence organisation, including those deployed in international military operations. It cooperates with MIVD and the Dutch National Cyber Security Centre (NCSC), which is subordinated to the Ministry of Security and Justice.¹²³

In case of large-scale cyber incidents, or upon the request of public authorities, the Dutch defence organisation will support the protection of public and private critical national infrastructure.¹²⁴ In practice this support will be provided by DefCERT, which cooperates with civilian authorities in the

coordination of cyber incident response and can be assigned to act in their support.¹²⁵ In addition,

In case of large-scale cyber incidents, or upon the request of public authorities, the Dutch defence organisation will support the protection of public and private critical national infrastructure

NCSC seconds a staff member to the Defence Cyber Command, which in return provides a staff member to NCSC.

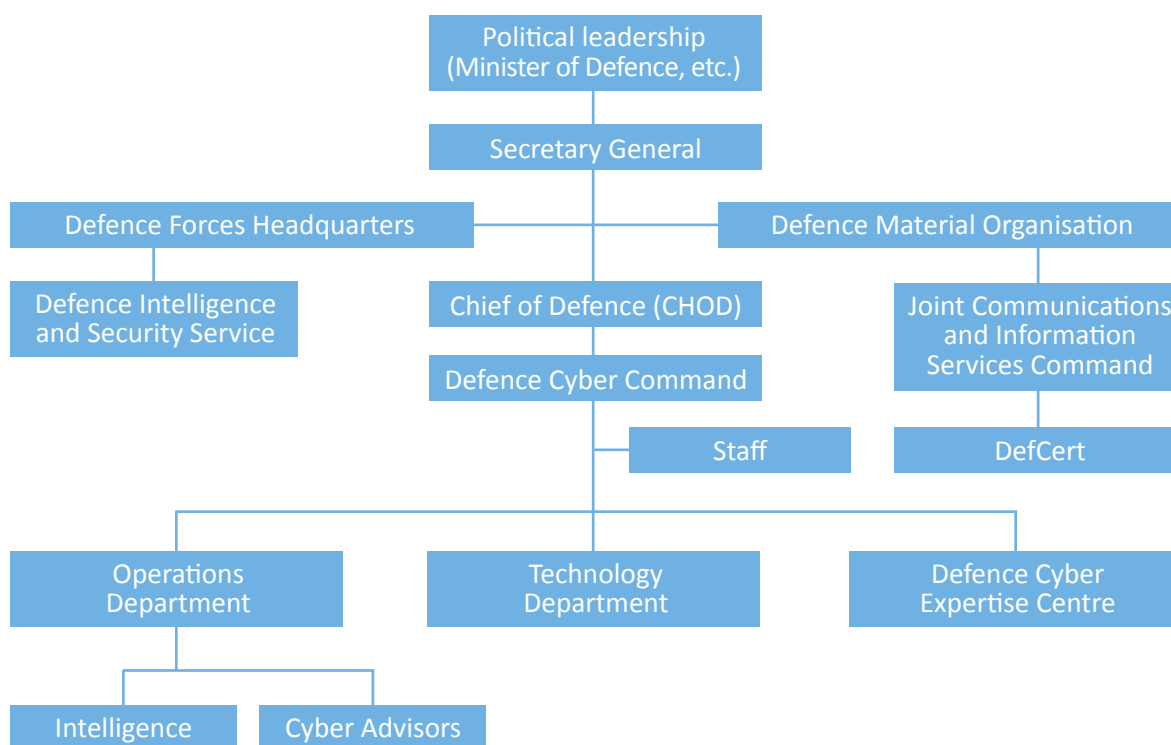


Figure 4. Defence Cyber Command, the Netherlands

¹²³ Ministry of Defence, "Defensie Computer Emergency Response Team," [Defence Computer Emergency Response Team], <https://www.defensie.nl/onderwerpen/cyber-security/defcert> (accessed November 10, 2018).

¹²⁴ National Coordinator for Security and Terrorism, *National Cyber Security Strategy 2: From Awareness to Capability*, 2013, p. 15, p. 21, p. 24, p. 32, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf> (accessed November 10, 2018).

¹²⁵ DefCERT has a Memoranda of Understanding with National Cyber Security Centre that requires mutual support and information sharing. Kadri Kaska, *National Cyber Security Organisation: the Netherlands*.

2.5. NORWAY: CYBER DEFENCE

Strategic Guidelines

Norway's first national-level cyber security strategy was published in 2003.¹²⁶ The latest version of the cyber security strategy dates from 2012; an updated version of it will be developed in 2018.¹²⁷ The strategy sets out priorities for all public authorities and does not make any explicit reference to the development of military cyberspace capabilities.¹²⁸ A strategic level document that describes the development of the armed forces' cyberspace capabilities was published by the Ministry of Defence in 2014; it also prescribes the development of defensive and offensive cyberspace operations in the armed forces.¹²⁹ According to these and other publicly available strategic documents, Norwegian cyberspace operations are performed in the armed forces as independent operations and in order to support land, air, sea, or joint operations.¹³⁰ Between 2018-2020, the defence sector's ICT management will be streamlined and the responsibilities of military CIRC (*Beskyttelse av kritisk infrastruktur*, BKI) will be expanded.¹³¹

¹²⁶ Ministry of Defence, *National Strategy for Information Security*, June 2013, https://www.regjeringen.no/globalassets/upload/kilde/mod/red/2000/0002/ddd/pdfv/249054-nasjonal_strategi_for_informasjonssikkerhet.pdf (accessed November 10, 2108).

¹²⁷ In September 2017, the "International Cyber Strategy for Norway" was published; however, the document does not include provisions for the development of the armed forces' cyber capabilities. Norwegian Ministry of Foreign Affairs, *International Cyber Strategy for Norway*, 2017, https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf (accessed November 10, 2018).

¹²⁸ The Ministry of Government Administration, Reform and Church Affairs, "Cyber Security Strategy for Norway," December 17, 2012. https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf (accessed November 10, 2018).

¹²⁹ Ministry of Defence, "Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren" [Policy on Information Security and Cyber Operations in the Defence Sector of the Ministry of Defence], March 1, 2014, <https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf?id=22346> (accessed November 10, 2018).

¹³⁰ Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 12.

¹³¹ Norwegian military CIRC is called the Centre for Critical Infrastructure Protection (*beskyttelse av kritisk infrastruktur*, BKI) and it is part of Cyber Defence. Ministry of Defence, "Prop. 1 S (2017 – 2018) Proposisjon til Stortinget (forslag til stortingsvedtak)" [Prop. 1 S (2017 - 2018) Proposition to the Storting (Proposal for a Parliamentary Resolution)], page 21, https://www.regjeringen.no/contentassets/2b306e220ea240178a0e0226ed9a04ff/no/pdfs/prp201720180001_fddddpdfs.pdf (accessed November 10, 2018).

Political Authorisation of International Deployments

The government decides on international deployments of military units.¹³²

Norwegian cyberspace operations are performed in the armed forces as independent operations and in order to support land, air, sea, or joint operations

Organisation

The Norwegian armed forces are divided into four military services: army, navy, air force, and the Home Guard (*Heimevernet*). The armed forces consist of 14 different departments and branches, including the Norwegian Armed Forces Cyber Defence (*Cyberforsvaret*, hereafter Cyber Defence). The Cyber Defence was established in September 2012 when the name of the Norwegian Defence Information Infrastructure organisation was changed and its status elevated to that of a standalone defence department or branch.¹³³ Cyber Defence constitutes a joint capability together with other supporting capabilities such as military intelligence, special operations, military police, logistics, medical services, etc.¹³⁴ The Commander of the Cyber Defence is directly subordinated to the CHoD. Cyber Defence consists of the following departments:¹³⁵

- 1) Cyber Defence CIS regiment, including the Cyber Defence Operations Centre;
- 2) Cyber Security Centre, including military CIRC;
- 3) Cyber Defence Weapons School;
- 4) Cyber Defence ICT Services;
- 5) Cyber Defence Base and Alarm Services.

In 2017 Cyber Defence' annual budget was approximately 1.86 million kronor (€197,000),

¹³² European Defence Agency, "Norwegian Defence 2013. Facts and Figures," p. 11, p. 150, <https://www.eda.europa.eu/docs/default-source/documents/norwegian-defence-2013.pdf> (accessed November 10, 2018).

¹³³ European Defence Agency, "Norwegian Defence 2013. Facts and Figures."

¹³⁴ Norwegian Armed Forces, "Norwegian Armed Forces in Transition," 2015, https://forsvaret.no/en/ForsvaretDocuments/Strategic_Defence_Review_2015_abridged.pdf (accessed November 10, 2018).

¹³⁵ Ministry of Defence, "Cyberforsvaret," [Cyber Defence], <https://forsvaret.no/cyberforsvaret> (accessed November 10, 2018).

or 5.5% of the annual defence budget. That year, its total workforce (civilian, professional military, and conscripts) was 1,230.¹³⁶

Cyber Defence supports the armed forces' freedom of action in the cyber domain

Functions

Cyber Defence supports the armed forces' freedom of action in the cyber domain.¹³⁷ It operates and maintains ICT-related military services and infrastructure, including Command and Control and other information networks, systems and platforms both at home and abroad; in addition, it plans and conducts defensive cyberspace operations.¹³⁸ The official functions include providing sensor and radar data, organising ICT-related training and exercises for the armed forces, and developing technological expertise.¹³⁹ It is not responsible for offensive cyberspace operations. Cyber defence-related procurement programmes are managed by the Norwegian Defence Materiel Agency.¹⁴⁰

Situational Awareness and Offensive Cyberspace Operations

ISR and offensive cyberspace operations are the responsibility of the Norwegian Intelligence Service (*Etterretningstjenesten*, E-tjenesten).¹⁴¹ Although E-tjenesten is part of the armed forces and falls under the CHoD, it provides services for the entire government apparatus – thus combining both military and foreign intelligence functions into a single organisation.¹⁴² Its main missions are to provide early warning about external threats – by gathering, processing, and analysing information related to foreign states, organisations, and individuals – and to support the operations of the armed forces at home

and abroad.¹⁴³ In the cyber field, the service performs the following tasks: providing early warning of cyber threats, contributing to cyber situational awareness as part of the Joint Cyber Coordination Centre, and coordinating cyberspace operations with the police, the Norwegian National Security Authority (NSM), Cyber Defence, and other relevant authorities as appropriate.¹⁴⁴

NSM supervises the safeguarding of information and infrastructure of national significance.¹⁴⁵ It is subordinated administratively to the Ministry of Defence, and additionally reports to the Ministry of Justice and the Police. In the area of cyber security, NSM is responsible for early warning, information sharing and coordination of the management of serious cyber-attacks against critical infrastructure or against vital services.¹⁴⁶ It provides notification of – and manages the responses to – data attacks against national critical infrastructure, and maintains a national security assessment picture.¹⁴⁷ Further tasks include gathering and analysing information relevant for Norway's protective security services, monitoring and penetrating information systems, carrying out technical surveillance countermeasures, and providing cryptosecurity.¹⁴⁸

¹³⁶ Norwegian Armed Forces, *Årsrapport*, [Annual Report], p. 102, https://forsvaret.no/fakta/_Forsvaret/Documents/Forsvarets_aarsrap_2017_utskriftsvennlig.pdf (accessed November 10, 2018).

¹³⁷ Ministry of Defence, "Cyberforsvaret."

¹³⁸ Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 17.

¹³⁹ Norwegian Armed Forces, "Other Departments," <https://forsvaret.no/en/organisasjon/other-departments> (accessed November 10, 2018).

¹⁴⁰ Norwegian Defence Materiel Agency, "We Equip the Norwegian Armed Forces," <https://forsvaret.no/forsvarsmateriell/en> (accessed November 10, 2018).

¹⁴¹ Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 5-6.

¹⁴² Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 5-6, p. 18.

¹⁴³ Norwegian Armed Forces, "Other Departments," Norwegian Armed Forces, "Etterretningstjenesten," <https://forsvaret.no/organisasjon/etterretningstjenesten> (accessed November 10, 2018).

¹⁴⁴ The Norwegian Joint Cyber Coordination Centre is a coordination mechanism between NSM, E-tjenesten, the Police Security Service, and the National Criminal Investigation Service (criminal police) that is activated in the event of very serious cyber-attacks. Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 18.

¹⁴⁵ Norway's national CIRC (NorCERT) is part of NSM. See Lilly Pijenburg Muller et al, *Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector* (Oslo: Norwegian Institute of International Affairs, 2018), https://brage.bibsys.no/xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y (accessed November 10, 2018).

¹⁴⁶ The Norwegian Intelligence Service, "Focus 2018," https://forsvaret.no/fakta/_Forsvaret/Documents/Fokus2018_engelsk_Enkeltstider_Godkjent_med.pdf (accessed November 10, 2018).

¹⁴⁷ Lilly Pijenburg Muller et al, *Cyber-weapons in International Politics*; Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 18.

¹⁴⁸ "Act of 20 March 1998 no. 10 Relating to Protective Security Services (the Security Act)", University of Oslo, <http://app.uio.no/ub/ujur/oversatte-lover/data/lov-19980320-010-eng.pdf> (accessed November 10, 2018). The Norwegian National Security Authority, "English," published April 23, 2014, <https://nsm.stat.no/english/> (accessed November 10, 2018);

Thus, both E-tjenesten and the NSM have a number of responsibilities in the areas of both defensive and offensive cyberspace operations.¹⁴⁹ In order to plan and conduct its defensive cyberspace operations, Cyber Defence must attain cyber situational awareness and cooperate closely with both of these organisations.

Assistance to the Civilian Authorities

The CHoD may provide assistance to civilian authorities in the area of cyber defence, in accordance with its statutory obligations.¹⁵⁰ However, Cyber Defence is currently not responsible for providing such assistance in the protection of critical national infrastructure against cyber incidents.¹⁵¹

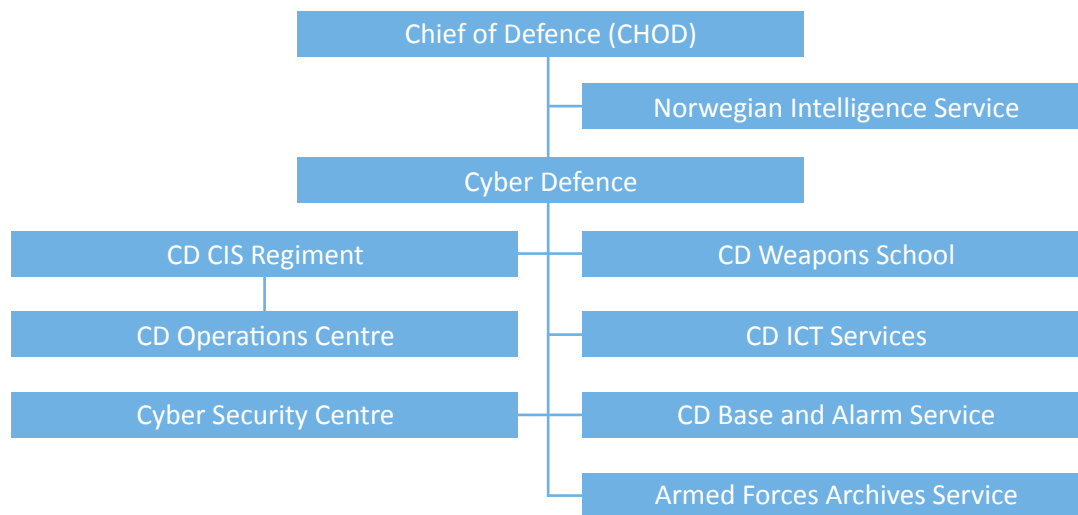


Figure 5. Cyber Defence, Norway

¹⁴⁹ It is beyond the scope of this study to determine whether E-tjenesten has the authority to conduct offensive operations whose purpose is the use of force.

¹⁵⁰ Ministry of Defence, "Forsvarsdepartementets retningslinjer," p. 19.

¹⁵¹ Per the new Security Act that is currently under consideration, the NSM— including the national CIRC NorCERT— has a supervisory role in preventing cyber attacks against critical national infrastructure or essential services. NSM and NorCERT, together with Sectoral Response Teams, assist private sector critical national infrastructure owners and providers in the management of a cyber incident. However, the national-level response to a major cyber-attack in the petroleum sector may be slow and insufficient. Lilly Pijnenburg Muller et al, *Cyber-weapons in International Politics*, p. 34; Ministry of Defence, "Prop. 1 S (2017 – 2018) Proposisjon til Stortinget (forslag til stortingsvedtak)," p. 21.

Table 1. Comparison of Cyber Commands or cyber forces in Estonia, Finland, Germany, Netherlands, Norway, and the United States

Country/Name of the cyber force	Estonia/ Cyber Command	Finland/ Cyber Division of C5 AGENCY	Germany/ CIR	Netherlands/ Defence Cyber Command	Norway/ Cyber Defence	United States/ USCYBERCOM
Type and size (full operational capability)	Cyber Command; 300	J6 with cyber defence component; 100-200	Functional Military Service; 14,500	Cyber Command	Defensive Cyberspace Operations, military CERT; 1,230	Cyber Command; 6,000
Subordination	CHOD	C5 Agency	Ministry of Defence	CHOD	CHOD	CHOD

Functions	Estonia	Finland	Germany	Netherlands	Norway	United States
Defend the country against serious cyber-attacks or assist civilian authorities in doing so	No	No	Yes	No (this function is performed by DefCERT)	No	Yes ¹⁵²
Defend military systems, networks, infrastructures, etc. against cyber threats	Yes	Yes	Yes	No (this function is performed by DefCERT)	Yes	Yes
Intelligence, Surveillance, Reconnaissance (Computer Network Exploitation)	No	No, but maintains situational awareness	Yes	Yes (signal intelligence is also provided by MIVD and JSCU)	No	Yes
Offensive Cyberspace Operations (Computer Network Attack)	Yes	Yes	Yes	Yes	No	Yes
Development of cyber effects for military operations; planning and executing standalone cyberspace operations	Yes	No	Yes	Yes	Only defensive cyberspace operations	Yes
Information Operations	Yes	No	Yes	No	No	No
Electronic Warfare	No	No	Yes	No	No	No
Mission Assurance	No	No	No	No	No	No (provided by military services)
Acquisition	No	No	No	No	No	Yes
Education, training, exercises	Yes	Yes	Yes	Yes	Yes	N/A
Workforce development (career paths, recruitment policies, etc.)	Yes	Yes	Yes	Yes	N/A	Yes
Political authorisation of offensive cyberspace operations	Parliament	President, on the proposal of the government	Parliament or in certain cases government	Government	Government	President. Decision can be delegated to lower levels. ¹⁵³

¹⁵² USCYBERCOM defends the country and critical national infrastructure “against cyberattacks of significant consequence.” See US Department of Defence, “All Cyber Mission Force Teams Achieve Initial Operating Capability,” October 24, 2016, <https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/> (accessed November 10, 2018).

¹⁵³ The US president authorises cyberspace operations intended to yield defensive or offensive cyber effects in information networks of other countries. This decision can be delegated to lower levels in the chain of command. USCYBERCOM is pre-authorized to conduct certain types of military cyberspace operations pursuant to decrees issued by operational commanders, the Secretary of Defence and the President. See Joint Chiefs of Staff, “Cyberspace Operations”; “US Cyber Operations Policy,” The Federation of American Scientists (FAS), <https://fas.org/irp/offdocs/ppd/ppd-20.pdf> (accessed November 10, 2018); Congress, “H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019,” Part I, Section 1621, <https://www.congress.gov/bill/115th-congress/house-bill/5515/text> (accessed November 10, 2018).

3. DISCUSSION

In this section, the reasons why countries decided to establish cyber commands or services are discussed while reviewing the anticipated advantages (including greater investment into cyber defence). Different national procedures of politically authorising international deployments, as well as differing organisational set-ups of cyber commands and their key functions are compared. Finally, policy recommendations in the areas of organisation and command, political authorisation of international deployments, key functions, as well as personnel policies and education, training, and exercise efforts are presented.

3.1. RATIONALE FOR ESTABLISHING A CYBER COMMAND

Only one subject matter expert argued that the rationale for the establishment of a cyber command was the need to prepare the armed forces for operating in the new operational domain. Instead, in the countries studied, the establishment of cyber commands (or military cyber service) was largely predicated by the need to centralise, consolidate, and streamline formerly fragmented capabilities and organisations, while eliminating overlapping roles and responsibilities.¹⁵⁴ This way, the armed forces can attain the objectives in the cyber and information domains set out in national strategic guidelines. Most experts expressed the same rationales promulgated in these concepts: for example, modernising the armed forces and its ICT infrastructure, networks and systems, as well as promoting innovation, augmenting

Instead, experts anticipated that the reorganisation of existing capabilities into a single organisation under a unified command will facilitate financial and other investment by prioritising the cyber domain at the strategic leadership level. The unified cyber command, in their view, concentrates the cyber defence and ICT expertise as well as expertise about operational planning and coordination of cyberspace operations.

It was suggested that an independent functional organisation under a country's CHoD allows for the development and implementation of non-traditional policies and helps solve challenges related to the lack of cyber defence workforce, overly long procurement time cycles that do not match the speed of technological development, inflexible career models for military cyber experts, and so forth. In sum, experts tended to believe that the founding of the new organisation *itself* augments the capability of the armed forces to operate in the cyber domain.

3.2. PRIORITISATION, INVESTMENT, COORDINATION

Changes to the traditional mindset of senior military leaders are needed if a cyber command is ultimately to be established. At the same time, as discussed above, the creation of independent cyber command was also perceived as a means of improving the status of cyber defence among the senior military leaders, which in turn increases investment in the domain. Similarly, the experts argue, it helps senior military leadership and operational commanders to understand the nature of cyber domain, as well as the role and advantages of integrating cyberspace operations in military operations.

Some experts underlined the importance of lean command and control for conducting cyberspace operations stemming from ubiquitous characteristics of cyberspace, its global reach and transaction speed. It was anticipated that the elevation of cyber commands to a position directly under national CHoDs will automatically grant the commander of cyber command greater authority pertaining to operations, personnel, equipment, force building, etc. As table 1 indicates, in Estonia, the Netherlands

The objective to project national power in and through cyberspace was not perceived as the key rationale for establishing a combatant command

knowledge and skills, etc. Thus, the objective to project national power in and through cyberspace was not perceived as the key rationale for establishing a combatant command.

¹⁵⁴ Examples of re-organisation are Germany, Estonia, and Norway.

and Norway cyber commands are subordinated directly to the CHoD, while in Germany and in Finland the command authority is more complex – potentially complicating or even delaying decision-making and coordination and de-conflicting with other military operations.¹⁵⁵

3.3. POLITICAL AUTHORISATION OF INTERNATIONAL DEPLOYMENTS

In terms of the geographical area of cyberspace operations, the Estonian and Finnish experts interviewed believe that their national cyber defence teams should focus on defending the homeland. However, this may not be feasible in practice because cyberspace is global, effective cyber defence requires “defending forward”, and participation in real-life international military operations will be valuable for skills development (as training cannot replace the experience of real battle).¹⁵⁶

Concerning international deployments of the armed forces generally they are confined to a limited time period within a designated geographic area of operations.¹⁵⁷ Among the five countries studied, in the Netherlands and Norway governments decide on the deployment of armed forces abroad, including their use of offensive cyberspace operations. In Germany the decision is made by the parliament, though in certain cases it can be made by the government as well. In Finland the president decides on a proposal which is made by the government, while in Estonia the parliament decides on a government proposal.

¹⁵⁵ In Finland the Chief of the Cyber Division is subordinated to the Director of the C5 Agency, who is subordinated to the Chief of the Armed Forces Headquarters, who is in turn subordinated to the CHoD. In Germany the CIR is subordinated to the Ministry of Defence, while strategic guidelines are provided by the Directorate-Generals of Cyber/IT and Strategy and Operations.

¹⁵⁶ For “defending forward” see Robert Chesney, “The 2018 DOD Cyber Strategy: Understanding ‘Defense Forward’ in Light of the NDAA and PPD-20 Changes,” *Lawfare*, September 25, 2018, <https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes> (accessed November 7, 2018).

¹⁵⁷ There are exceptions to this rule. For example, in Estonia the parliament determines for each year the limit number of active servicemen who may participate in international military operation led by NATO, its ally, the EU or UN upon contributing thereto for the first time. See “National Defence Act,” paragraph 34, 4.

However, in case of the intent to deploy defensive and offensive cyberspace operations, which require secrecy for their success, public discussions are not possible. Moreover, effective cyberspace operations cannot be limited in time and space and must be executed at short notice.

The contemporary political authorisation processes and procedures in democratic countries should be examined – and if needed, also revised – to enable delegation of decision-making to lower levels of political authority

For these reasons the contemporary political authorisation processes and procedures in democratic countries should be examined – and if needed, also revised – to enable delegation of decision-making to lower levels of political authority. In certain cases, instead of the parliament the government, minister of defence, CHoD, or head of Cyber Command might be better placed to make such a decision. Many countries have solved this challenge by allowing for the pre-authorisation of certain types of military operations.¹⁵⁸

3.4. ORGANISATION

Among the above country case studies, the Netherlands has a cyber command in the strict meaning – that is, one which has the capability and authority to direct and control the full spectrum cyberspace operations: defensive, ISR and offensive cyberspace operations. The German CIR is a military cyber and information domain service that has the same capabilities and authority not only in cyberspace, but also regarding electronic warfare and information

¹⁵⁸ For example, USCYBERCOM may conduct certain types of military cyberspace operations on the basis of decrees issued by operational commanders, the Secretary of Defence, and the President that pre-authorise certain types of cyber activities and operations. See “Cyberspace Operations.” Moreover, in August 2018 Presidential Policy Directive PPD-20 was rescinded, eliminating the inter-agency vetting process used for approving and deconflicting cyberspace operations, and thereby enabling the Commander of USCYBERCOM to decide on cyberspace operations without prior approval by other federal government stakeholders. Robert Chesney, “Offensive Cyber Operations and the Interagency Process: What’s at Stake With the New Trump Policy,” *Lawfare*, August 16, 2018, <https://www.lawfareblog.com/offensive-cyber-operations-and-interagency-process-whats-stake-new-trump-policy> (accessed November 10, 2018).

operations.¹⁵⁹ The Estonian cyber command likewise includes an information operations capability, but it does not have an ISR component. The Cyber Defence in Norway does not constitute cyber command in the above strict meaning, because offensive cyberspace operations are directed and controlled by the E-tjenesten, Norway's intelligence service. The Finnish Cyber Division is responsible for cyber defence and situational awareness, as well as for cyber force building matters (such as education, training and exercises), but other departments in the Defence Forces and its headquarters also share these responsibilities. Thus, in the Finnish case the centralisation, consolidation, and streamlining of these fragmented existing capabilities would likely improve efficiency, reduce costs, and clarify roles and responsibilities to avoid duplications. This applies also to the area of intelligence collection, where the Cyber Division depends on information collected by other defence organisations (PVTIEDL and the Intelligence Division of the Finnish Defence Forces Headquarters), and to the area of operational planning (the Operations Division of the Defence Forces Headquarters).

All countries except Finland have a Cyber Operations Centre (in Estonia it includes an information operations component). Germany and the Netherlands have integral intelligence or ISR and software development components in their cyber commands. All countries except the Netherlands have military CIRC within their cyber commands (in Finland CIRC functions are separately part of the C5 Agency). All countries have some components (schools and expertise centres) responsible for cyber defence education, training, and exercises.

In summary, as table 1 indicates, while there are many commonalities among the countries pertaining to command authority and organisational components (departments, centres, schools, battalions, etc.) there are also great differences. The best organisational model for a cyber command depends on the range of variables in the particular country, such as existing cyber defence, ICT, and intelligence organisations in the armed forces, available financial resources and manpower (country size), strategic priorities

(expeditionary operations versus territorial defence), as well as the broader strategic and military culture, historical civil-military relations, and traditions of democratic oversight. However, as with other military organisations, the leaner the organisational structure and command authority, the clearer the roles and responsibilities, and the more resources allocated, the greater the opportunities to develop state-of-art cyberspace operations capabilities and integrate these in military operations.

Comparing the five countries, the Netherlands has the leanest organisational structure consisting of only three departments, of which two (Operations and Technology) are directly responsible for the development of cyberspace operations and capabilities. Germany, Estonia, and Norway have integrated a broader range of components that may indirectly sustain these efforts through force-building (for example, the SSB [Support and Signal Battalion] in Estonia) or through ensuring cyber security of the armed forces such as CIRC, ICT services, CIS support centres, etc. The advantages of a lean organisation is greater agility and flexibility, fast decision-making and deployment, and clarity about how investment is spent, while the advantages of larger organisations are the reducing of overlapping responsibilities, joint command of resources, as well as the potential deterrent effect of having a larger number of personnel in the cyber command.

3.5. FUNCTIONS

As discussed above and as table 1 indicates, only the German and Dutch cyberspace organisations of the armed forces conduct all three types of cyberspace operations (defensive, ISR and offensive cyberspace operations) and thus can be categorised as full-fledged cyber commands in the strict sense as identified above.¹⁶⁰ In addition, the Estonian Cyber Command and Finnish Cyber Division direct and control defensive and offensive cyberspace operations. Estonia, Finland, Germany, and the Netherlands all acknowledge offensive cyberspace capabilities of the armed forces, prepare for planning and executing cyberspace operations and integrating cyberspace effects

¹⁵⁹ See footnote 20 for the explanation that the German cyberspace organisation constitutes a hybrid of a service and a combatant command.

¹⁶⁰ The German cyberspace organisation constitutes a hybrid of a service and a combatant command.

into traditional military operations. Thus, concerning these functions, the four countries are similar to the USCYBERCOM.¹⁶¹

Estonia, Finland, Germany, and the Netherlands all acknowledge offensive cyberspace capabilities of the armed forces, prepare for planning and executing cyberspace operations and integrating cyberspace effects into traditional military operations

As shown in table 1, a majority of cyber commands (Estonia, Finland, the Netherlands, and Norway) do not have a legal mandate to defend critical national infrastructure or assist civilian authorities, which can be explained by the existence of strong civilian authorities that coordinate inter-agency responses to serious cyber incidents or cyber attacks against the country. In the Netherlands, DefCERT is assigned to act in support of civilian authorities. In Estonia the Cyber Defence Unit of the Defence League can be assigned to ensure the cyber security of state functions and vital services, including those in the private sector.¹⁶² In all countries comprehensive approach – whole-of-government and whole-of-society cooperation – as well as international cooperation are key responsibilities of the armed forces. Finland, Germany, and the Netherlands have established comprehensive personnel policies for military cyber experts (including recruitment, specific career paths, incentives, etc.) as well as policies on cyber defence education, training, and exercises. The Netherlands, for example, is creating and refining specific occupational profiles for cyber personnel, and in the near future plans to determine education and

training requirements for them.¹⁶³ The Estonian and Norwegian cyberspace organisations have similarly substantial responsibilities in the development of cyber defence personnel for the armed forces, in particular through the preparation of reserve forces. These and other best practices should be collected and shared through NATO and EU cyber security education and training events and platforms.¹⁶⁴

Interestingly, none of the cyber commands has the explicit responsibility to ensure mission assurance or the direct authority to acquire equipment and capabilities for cyber forces. In the future this may change, for example, in 2017 USCYBERCOM acquired limited acquisition authority in order to enable faster and flexible procurement procedures.¹⁶⁵ Furthermore, it was revealed last year that in 2015 USCYBERCOM did not have “appropriate authorities to effectively oversee and direct offensive capability development”; accordingly, it was suggested that the cyber commanders should have authority to decide the development of cyberspace capabilities and to oversee their application, integration, and execution.¹⁶⁶

¹⁶¹ The efforts of NATO allies to conduct national cyberspace operations and integrate cyberspace effects could be supported by the NATO cyber doctrine that is expected to be issued in 2019. Germany and the Netherlands are planning to develop national-level cyber defence doctrine, and they could share their best practices in doing so with other NATO nations. Robin Emmot, “NATO Mulls ‘Offensive Defense’ with Cyber Warfare Rules,” *Reuters*, November 30, 2017, <https://www.reuters.com/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4> (accessed November 10, 2018).

¹⁶² Kadri Kaska, Anna-Maria Osula, and Jan Stinissen, *The Cyber defence Unit of the Estonian Defence League. Legal, Policy, and Organisational Analysis*. (Tallinn: NATO CCD COE, 2013), https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (accessed November 10, 2018). Government, “Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel.”

¹⁶³ The US Marine Corps has created the following cyberspace operations occupational profiles: general cyberspace officers, cyberspace warfare development officers, defensive cyberspace weapons officers, offensive cyberspace weapons officers, cyberspace defensive operators, cyberspace effects operators, and cyber operations chiefs. See the United States Marine Corps, “Establishment of the Cyberspace 1700 Occupational Field (OCCFLD), January 3, 2018, <http://www.marines.mil/News/Messages/Messages-Display/Article/1454562/establishment-of-the-cyberspace-1700-occupational-field-occfld/> (accessed November 10, 2018).

¹⁶⁴ In international military operations, the RAND Corporation distinguishes the following cyberspace operations occupational profiles at the tactical level: forward deployed cyber technicians, cyber planners, cyber experts, and reach back experts. See Isaac R. Porche III, Christopher Paul, et.al., *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below*, (Santa Monica: Rand Corporation, 2017), DOI: 10.7249/RR1600.

¹⁶⁵ The Fiscal Year 2016 National Defence Authorization Act granted USCYBERCOM the authority to acquire, develop, and sustain equipment and capability related to cyberspace operations. “U.S. Cyber Command flexes new acquisition muscle,” October 12, 2017, <https://www.cybercom.mil/Media/News/News-Display/Article/1341294/us-cyber-command-flexes-new-acquisition-muscle/> (accessed November, 2018).

¹⁶⁶ Shaun Waterman, “Cyber Command Lacks Authorities, Capabilities, Pentagon Watchdog Says,” *Cyberscoop*, September 7, 2017, <https://www.cyberscoop.com/cyber-command-lacks-authorities-capabilities-pentagon-watchdog-says/> (accessed November 10, 2018).

POLICY RECOMMENDATIONS

Organisation and Command

In every military function, a lean and agile organisation brings a number of advantages; however, case studies demonstrate that many countries have integrated those functions under cyber commands, service or division that are not directly necessary for integrating cyberspace

There exists no universal best practice for establishing a cyber command

effects into military operations and conducting standalone cyberspace operations. There exists no universal best practice for establishing a cyber command, although the lean organisation of the Netherlands can be considered as a model for small countries with limited human and financial resources. Moreover, as these case studies demonstrate, the division of roles and responsibilities among cyber commands, military operations divisions, and intelligence divisions may not be clearly identified and command authority may be complicated, which can hinder the operational effectiveness and decision-making. Accordingly, the commander of cyber command could be immediately subordinated to the CHoD (in peacetime) or the Joint/Operational Commander (during operations).

Political Authorisation of International Deployments

Democratic countries adhere to the principle of democratic oversight of military, intelligence, and law enforcement; however, in certain cases regulations and procedures (for example, the requirement for parliamentary authorisation for cyberspace operations) should be reconsidered. On the one hand, democratic oversight, checks and balances, as well as the risk of conflict escalation, should be retained at the strategic-political level; at the same time, however, cyber commands must have real-time intelligence to prepare the operational environment, including persistent presence outside the designated geographical area of military operations. In certain cases, decision-making authority should be delegated to the lower levels of political authority (for example, the government, minister of defence, CHoD, or Commander of Cyber Command).

Defensive, ISR and Offensive Cyberspace Operations

Intelligence collection can either be a function of cyber command (in Germany and the Netherlands), and/or provided by intelligence services (Estonia, Finland, Norway). The planning and execution of cyberspace operations must be coordinated, de-conflicted, integrated, and synchronised with traditional military operations, including electromagnetic spectrum activities and information operations.

For example, the Netherlands and the United States have created inter-agency intelligence units for improving information and intelligence sharing, coordination, and situational awareness.¹⁶⁷

Other Functions

The primary functions of cyber commands are planning and conducting defensive and offensive cyberspace operations and ISR cyberspace operations, as well as ensuring the cyber security of military networks, systems, and infrastructures (many cyber commands encompass CIRC functions as well).

Germany has electronic warfare and information operations capabilities in its cyber and information domain service CIR. In the future, cyber commands should increasingly integrate these disciplines. For example, the UK and US have integrated electronic warfare and information operations with military cyberspace capabilities, as reflected in their operational-level planning doctrines.¹⁶⁸

The interviewed experts did not believe that support to civilian authorities in defending small countries against cyber-attacks is essential, but did recommend improvements to civil-military cooperation in general, for example by organising regular whole-of-society cyber defence exercises.

¹⁶⁷ In May 2018 an operational-level Integrated Cyber Centre/ Joint Operations Centre was established in the US that enables real-time situational awareness, coordination, and de-conflicting of cyberspace operations across federal agencies and with foreign partners. The Centre hosts representatives of USCYBERCOM, the National Security Agency, other US federal agencies, and US allies. Mark Pomerleau, "Cyber Command, NSA Open New \$500 Million Operations Center," *Fifth Domain*, May 7, 2018, <https://www.fifthdomain.com/dod/cybercom/2018/05/07/cyber-command-nsa-open-new-500-million-operations-center/> (accessed November 10, 2018).

¹⁶⁸ Joint Chiefs of Staff, "Cyberspace Operations."

Inter-agency cooperation agreements and mechanisms with national and allied intelligence services and other cyber commands should be concluded, in particular in the area of early-warning and intelligence.

NATO and EU countries should share best practices in designing career paths for cyber military personnel and in educating and training their military and civilian staff as a whole

Personnel Policies, Education, Training and Exercises Efforts

Some experts argue that because traditional military services do not have core competencies in cyberspace operations, tasks such as recruiting, training and equipping of cyber personnel should be conducted by functional cyber services or commands.¹⁶⁹ Nevertheless, NATO and EU countries should share best practices in designing career paths for cyber military personnel and in educating and training their military and civilian staff as a whole.

¹⁶⁹ See David Barno and Nora Bensahel, "Strategic Outpost Debates a Cyber Corps," *War on the Rocks*, February 20, 2018, <https://warontherocks.com/2018/02/strategic-outpost-debates-cyber-corps/> (accessed November 10, 2018).

LIST OF REFERENCES

- [illegible]

- . “Operationeel. Defensie Cyber Commando” [Operational. Defence Cyber Command]. Vereniging van Officiëren van de Verbindingsdienst [Association of Signal Corps Officers]. <https://vovklicl.nl/intercom/2016/1/22.pdf>. Accessed November 10, 2018.

Government (Estonia). “Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel” [Requirements and Order of Engaging the Defence League in Ensuring Cyber Security]. Regulation no. 108. July 3, 2014. <https://www.riigiteataja.ee/akt/110072014003>. Accessed November 7, 2018.

- . “Kaitseväge põhimäärus” [Statute of the Defence Forces]. Regulation no. 45. June 21, 2018. <https://www.riigiteataja.ee/akt/128062018008>. Accessed November 7, 2018.

Government of the Netherlands. *2014 Annual Report Netherlands Defence Intelligence and Security Service*. <https://www.government.nl/documents/annual-reports/2015/07/21/2014-annual-report-netherlands-defence-intelligence-and-security-service>. Accessed November 10, 2018.

- . “The Constitution of the Kingdom of the Netherlands 2008.” <https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008>. Accessed November 10, 2018.

Hackett, James, ed. *The Military Balance: The Annual Assessment of Global Military Capabilities and Defence Economics*. London: Routledge & The International Institute for Strategic Studies, 2017.

Headquarters of the Estonian Defence Forces. “Headquarters.” <http://www.mil.ee/en/defence-forces/Headquarters-of-the-Estonian-Defence-Forces>. Accessed November 7, 2018.

- . “Kaitseväge peastaabi põhimäärus” [Statute of Headquarters of the Estonian Defence Forces]. CHoD Decree no. 149, July 9, 2018. <http://www.mil.ee/et/kaitsevagi/organisatsioon/oigusaktid>. Accessed November 7, 2018.
- . “Küberväejuhatuse põhimäärus” [Statute of Cyber Command]. CHoD decree no. 149, July 9, 2018. <http://www.mil.ee/UserFiles/sisu/kaitsevagi/organisatsioon/kv%20oigusaktid/Kybervaejuhatuse%20pohimaaus.pdf>. Accessed November 7, 2018.

Headquarters, Department of the Army (United States). “Cyber Electromagnetic Activities.” FM 3-38. February 12, 2014. <https://fas.org/irp/doddir/army/fm3-38.pdf>. Accessed October 10, 2018.

Healy, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, Va.: Cyber Conflict Studies Association, 2013.

“ICDS seminar with General Riho Terras and Major-General Martin Herem.” Tallinn. International Centre for Defence and Security. November 5, 2018.

Information System Authority. *Annual Cyber Security Assessment 2018*. Tallinn, 2018. <https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf>. Accessed November 5, 2018.

Joint Chiefs of Staff. “Cyberspace Operations.” Joint Publication (JP) 3-12. June 8, 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930. Accessed October 9, 2018.

Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis*. Tallinn: NATO CCD COE, 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf. Accessed October 16, 2018.

Kaska, Kadri. *National Cyber Security Organisation: the Netherlands*. Tallinn: NATO CCD COE, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf. Accessed November 10, 2018.

Kiesel, Heiner. “Bundeswehr Cybersecurity Center Trains Elite Counterhackers.” *Deutsche Welle*. April 1, 2018. <http://www.dw.com/en/bundeswehr-cybersecurity-center-trains-elite-counterhackers/a-43210036>. Accessed November 10, 2018.

Kodar, Erki. Presentation at the NATO cyber symposium NIAS’17. Mons, Belgium. October 17-19, 2017. <https://www.youtube.com/watch?v=PKC-nWRfz4>. Accessed November 5, 2018.

Königsmark, Stefan. “Wachstum steuern – der Aufwuchs aus organisatorischer Sicht” [Controlling Growth – Growth from the Organisational Perspective]. *Sonderausgabe - Cyber- und Informationsraum, Europäische Sicherheit & Technik* [Special Edition - Cyber and Information Domain, European Security & Technology]. Bonn: Mittler Report Verlag, 2018.

- Koot, Matthijs. "The Dutch Defense Cyber Command: A New Operational Capability." Matthijs R. Koot's Notebook. <https://blog.cyberwar.nl/2014/10/the-dutch-defense-cyber-command-a-new-operational-capability-colonel-hans-folmer-2014/>. Accessed November 10, 2018.
- Leinhos, Ludwig. "Planung und Umsetzung der Abteilung Cyber/IT (CIT) und des OrgBer Cyber- und Informationsraum (CIR)" [Planning and Implementation of the Cyber/IT (CIT) Department and the OrgBer Cyber and Information Domain (CIR)]. https://www.afcea.de/fileadmin/user_upload/News/Dokumente/Vortrag_KO_IT-Ta-gung_Leinhos_LtrAufbStab_CyberInfoR.pdf. Accessed November 10, 2018.
- López de Turiso y Sánchez, Javier. "Evolucion del Concepto de Ciberdefensa" [Evolution of the Concept of Cyber Defence]. Third Cyber Defence Symposium of the Spanish Joint Cyber Defence Command "Military Operations in Cyberspace." May 24, 2018. <https://jornadasciberdefensa.es/2018/programa/255/es>. Accessed October 5, 2018.
- "Luik: Eesti on vajadusel valmis andma oma kübervõimed NATO käsutusse" [Luik: Estonia is Prepared to Give Its Cyber Capabilities to NATO, If Needed]. *Eesti Rahvusringhääling (ERR)*. October 4, 2018. <https://www.err.ee/866519/luik-eesti-on-vajadusel-valmis-andma-oma-kubervoimed-nato-kasutusse>. Accessed November 5, 2018.
- Mäekivi, Mirjam. "Galerii: Eesti küberväejuhatuse asus tööle" [Gallery: Estonian Cyber Command Begins Operation]. *Eesti Rahvusringhääling (ERR)*. <https://www.err.ee/850643/galerii-eesti-kubervaejuhatuse-asus-toole>. Accessed November 5, 2018.
- McKenzie, Paul. *NATO Joint Air Power and Offensive Cyberspace Operations*. Kalkar: The Joint Air Power Competence Centre, November 2017. https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf. Accessed November 10, 2018.
- Ministry of Economic Affairs and Communications. "Riigi Infosüsteemi Ameti põhimäärus." [Statute of the Information System Authority]. Regulation no. 28, April 25, 2011. <https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv>. Accessed November 7, 2018.
- Ministry of Defence (Estonia). "NATO Investing in the Development of Estonian Cyber Range." June 14, 2016. <http://www.kmin.ee/en/news/nato-investing-development-estonian-cyber-range>. Accessed October 5, 2018.
- . "The National Defence Development Plan 2017-2026." <http://www.kaitseministeerium.ee/riigikaitse2026/arengu-kava/eng/>. Accessed November 5, 2018.
- . Last modified March 14, 2018. <http://www.kaitseministeerium.ee/en/organisation-contacts/ministry-defence>.
- Ministry of Defence (Finland). "Act of Military Crisis Management." March 31, 2006. <http://www.finlex.fi/en/laki/kaan-nokset/2006/en20060211.pdf>. Accessed November 7, 2018.
- . "Kysymyksiä ja vastauksia toimittajille sotilastiedustelulainsäädäntöön liittyen." [Questions and Answers to Editors About Military Intelligence Legislation]. https://www.defmin.fi/ajankohtaista/luonnos_hallituksen_esitykseksi_laiksi_sotilastiedustelutoiminnasta_ja_eraiksi_siihen_liittyviksi_laeiksi. Accessed November 10, 2018.
- Ministry of Defence (Netherlands). "A Look at the Defence News, 2 – 8 May." May 10, 2016, <https://english.defensie.nl/latest/news/2016/05/10/a-look-at-the-defence-news-2-%E2%80%93-8-may>. Accessed November 10, 2018.
- . "Central Staff." <https://english.defensie.nl/organisation/central-staff>. Accessed November 10, 2018.
- . "Defence Cyber Command." <https://english.defensie.nl/topics/cyber-security/cyber-command>. Accessed November 10, 2018.
- . "Defensie Computer Emergency Response Team" [Defence Computer Emergency Response Team]. <https://www.defensie.nl/onderwerpen/cyber-security/defcert>. Accessed November 10, 2018.
- . "Netherlands Defence Intelligence and Security Service." https://fas.org/irp/world/netherlands/mivd_brochure.pdf. Accessed November 10, 2018.
- . *The Defence Cyber Strategy*. The Hague, 2012. https://ccdcoe.org/sites/default/files/strategy/NDL-Cyber_Strategy-Eng.pdf. Accessed November 10, 2018.
- . "The Defence Cyber Strategy." 2015. <https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy>. Accessed November 10, 2018.

- Ministry of Defence (Norway). "Cyberforsvaret." [Cyber Defence] <https://forsvaret.no/cyberforsvaret>. Accessed November 10, 2018.
- . "Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren" [Policy on Information Security and Cyber Operations in the Defence Sector of the Ministry of Defence]. March 1, 2014. <https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf?id=22346>. Accessed November 10, 2018.
- . *National Strategy for Information Security*. Oslo, June 2013. https://www.regjeringen.no/globalassets/upload/kilde/mod/red/2000/0002/ddd/pdfv/249054-nasjonal_strategi_for_informasjonssikkerhet.pdf. Accessed November 10, 2018.
- . "Prop. 1 S (2017 – 2018) Proposisjon til Stortinget (forslag til stortingsvedtak)" [Prop. 1 S 2017 - 2018) Proposition to the Storting (Proposal for a Parliamentary Resolution)]. https://www.regjeringen.no/contentassets/2b306e220ea240178a0e0226ed9a04ff/no/pdfs/prp201720180001_fdddpdfs.pdf. Accessed November 10, 2018.
- Ministry of Defence (Singapore). "Fact Sheet: SAF C4 Command Integrates C4 and Cyber Defence Capabilities." June 30, 2017. <https://www.mindef.gov.sg>. Accessed October 5, 2018.
- Ministry of Economic Affairs and Communications. *Cyber Security Strategy 2014-2017*. Tallinn, 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf. Accessed November 5, 2018.
- Ministry of Finance. "2017. aasta riigieelarve seaduse seletuskiri" [Explanatory Note for the 2017 State Budget]. <https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigieelarve-ja-majandus/riigieelarve-ja-majandusulevaated>. Accessed October 6, 2018.
- . "2018. aasta riigieelarve seaduse seletuskiri" [Explanatory Note for the 2018 State Budget]. <https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigieelarve-ja-majandus/riigieelarve-ja-majandusulevaated>. Accessed October 6, 2018.
- Ministry of the Interior. "Civilian intelligence legislation would improve Finland's national security." Press Release 9/2018. January 25, 2018. https://intermin.fi/en/artikkeli/-/asset_publisher/siviilitiedustelulaki-parantaisi-suomen-kansallista-turvallisuutta. Accessed November 10, 2018.
- National Coordinator for Security and Terrorism. *National Cyber Security Agenda: A cyber secure Netherlands*. The Hague, July 9, 2018. https://english.nctv.nl/binaries/CSAgenda_EN_def_web_tcm32-339827.pdf. Accessed November 10, 2018.
- . *National Cyber Security Strategy 2: From Awareness to Capability*. The Hague, 2013. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf>. Accessed November 10, 2018.
- National Cyber Security Centre. "National Cyber Security Strategy 2." <https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html>. Accessed November 10, 2018.
- North Atlantic Treaty Organisation Standardisation Agency. *NATO Glossary of Terms and Definitions (English and French)*. AAP-06. Brussels: North Atlantic Treaty Organisation Standardisation Agency, 2017.
- Norwegian Armed Forces. *Årsrapport* [Annual Report]. Oslo, 2017. https://forsvaret.no/fakta/_ForsvaretDocuments/Forsvarets_aarsrap_2017_utskriftsvennlig.pdf. Accessed November 10, 2018.
- . "Etterretningstjenesten" [Intelligence Service]. <https://forsvaret.no/organisasjon/etterretningstjenesten>. Accessed November 10, 2018.
- . *Norwegian Armed Forces in Transition*. Oslo, 2015. https://forsvaret.no/en/ForsvaretDocuments/Strategic_Defence_Review_2015_abridged.pdf. Accessed November 10, 2018.
- . "Other Departments." <https://forsvaret.no/en/organisation/other-departments>. Accessed November 10, 2018.
- Norwegian Defence Materiel Agency. "We Equip the Norwegian Armed Forces." <https://forsvaret.no/forsvarsmateriell/en>. Accessed November 10, 2018.
- Norwegian Ministry of Foreign Affairs. *International Cyber Strategy for Norway*. Oslo, 2017. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf. Accessed November 10, 2018.

- O'Dwyer, Gerard. "The Threat to Finland's Cyberdefense? Private-sector Salaries." *Fifth Domain*. February 5, 2018. <https://www.fifthdomain.com/international/2018/02/05/the-threat-to-finlands-cyberdefense-private-sector-salaries/>. Accessed November 7, 2018.
- "Operation Glowing Symphony." USCYBERCOM OPORD 16-0188. June 27, 2018. <https://www.documentcloud.org/documents/4624362-Cybercom-Operation-Glowing-Symphony-Documents.html>. Accessed November 5, 2018.
- Parliament (Estonia). "National Defence Act." Passed on February 11, 2015. <https://www.riigiteataja.ee/en/eli/ee/517112015001/consolide/current>. Accessed November 5, 2018.
- . "Security Authorities Act." Passed on December 12, 2000. <https://www.riigiteataja.ee/en/eli/521062017015/consolide>. Accessed November 7, 2018.
- . "The Estonian Defence League Act." Passed on February 28, 2013. <https://www.riigiteataja.ee/en/eli/530042018001/consolide>. Accessed November 5, 2018.
- . "Cybersecurity Act." Passed on May 9, 2018. <https://www.riigiteataja.ee/en/eli/523052018003/consolide>. Accessed November 7, 2018.
- Parliament Defence Committee (Finland). "Valiokunnan mietintö" [Committee's Consideration] PuVM 4/2017 vp – VNS 3/2017 vp. https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/PuVM_4+2017.pdf. Accessed November 7, 2018.
- Pijnenburg Muller, Lilly, Lars Gjesvik, and Karsten Friis. *Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector*. Oslo: Norwegian Institute of International Affairs, 2018. https://brage.bibsys.no/xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y. Accessed November 10, 2018.
- Pomerleau, Mark. "Cyber Command, NSA Open New \$500 Million Operations Center." *Fifth Domain*. May 7, 2018. <https://www.fifthdomain.com/dod/cybercom/2018/05/07/cyber-command-nsa-open-new-500-million-operations-center/>. Accessed November 10, 2018.
- Porche III, Isaac R., Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below*. Santa Monica: Rand Corporation, 2017. DOI: 10.7249/RR1600.
- Prime Minister's Office. *Government's Defence Report*. Helsinki: February 6, 2017. https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf. Accessed November 7, 2018.
- "Puolustusvoimat on moninkertaistamassa kyberyksikkönsä koon – "Suorituskykyämme testataan joka päivä" [Defence Forces Multiply Size of Their Cyber Unit: 'Our Capabilities Are Tested Daily']. *Yle*. May 30, 2016. <https://yle.fi/uutiset/3-8906483>. Accessed November 7, 2018.
- "Puolustusvoimat perustaa uuden kyberyksikön – hybridisotiin varaudutaan vahvistamalla verkkopuolustusta" [Defence Forces Establish a New Cyber Unit – Fostering Network Defence in Preparation for Hybrid Wars]. *Yle*. September 25, 2014. <https://yle.fi/uutiset/3-7491555>. Accessed November 7, 2018.
- Review Committee on the Intelligence and Security Services. "Annual report CTIVD 2017." <https://english.ctivd.nl/documents/annual-reports/2018/05/23/index>. Accessed November 10, 2018.
- . "Review Report on the Use of the Investigatory Power to Hack by the AIVD and the MIVD in 2015." <https://english.ctivd.nl/latest/news/2017/10/20/index>. Accessed November 10, 2018.
- . "Update website CTIV." <https://english.ctivd.nl/latest/news/2018/05/01/index>. Accessed November 10, 2018.
- Secretariat of the Security Committee. *Finland's Cyber Security Strategy*. Helsinki: January 21, 2013. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf. Accessed November 7, 2018.
- Shalal, Andrea, and Thomas Escritt. "In Cyber, Germany Needs to Counter-attack, Minister Says." *Reuters*. July 24, 2018. <https://uk.reuters.com/article/uk-germany-espionage-cyber/in-cyber-germany-needs-to-counter-attack-minister-says-idUKKBN1KE0YG>. Accessed November 10, 2018.
- Shalal, Andrea. "German Spy Agencies Want Right to Destroy Stolen Data and 'Hack Back'." *Reuters*. October 5, 2017. <https://www.reuters.com/article/us-germany-cyber/german-spy-agencies-want-right-to-destroy-stolen-data-and-hack-back-idUSKBN1CA1IN>. Accessed November 10, 2018.


- Skierka, Isabel. "Bundeswehr: Cyber Security, the German way" *Digital Frontiers*. October 20, 2016. <https://www.orfonline.org/expert-speak/bundeswehr-cyber-security-the-german-way/>. Accessed November 10, 2018.
- Smeets, Max, and Herbert Lin. "Offensive Cyberspace Capabilities: To What Ends?" in T. Minarik, R. Jakschis, L. Lindström, eds. *10th International Conference on Cyber Conflict Cycon X: Maximising Effects*. Tallinn: NATO CCD COE Publications, 2018. pp. 55-72. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2018_Full_Book.pdf. Accessed November 10, 2018.
- The Federation of American Scientists (FAS). "US Cyber Operations Policy." <https://fas.org/irp/offdocs/ppd/ppd-20.pdf>. Accessed November 10, 2018.
- The Finnish Defence Forces. "Defence Command Finland." <http://puolustusvoimat.fi/en/about-us/defence-command>. Accessed November 7, 2018.
- . "Defence Command Intelligence Division." <https://puolustusvoimat.fi/en/intelligence-division>. Accessed November 10, 2018).
- . "Finnish Defence Forces C5 Agency." <http://puolustusvoimat.fi/en/about-us/c5-agency>. Accessed November 7, 2018.
- . "Pääesikunnan johtamisjärjestelmäosasto" [The Finnish Defence Forces Headquarters Management System Department]. <http://puolustusvoimat.fi/tietoa-meista/paaesikunta/johtamisjarjestelmaosasto>. Accessed November 7, 2018.
- The Ministry of Government Administration, Reform and Church Affairs. *Cyber Security Strategy for Norway*. Oslo, December 17, 2012. https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf. Accessed November 10, 2018.
- The Norwegian Intelligence Service. "Focus 2018." https://forsvaret.no/fakta/_ForsvaretDocuments/Fokus2018_engelsk_Enkeltider_Godkjent_med.pdf. Accessed November 10, 2018.
- The Norwegian National Security Authority. "English." April 23, 2014. <https://nsm.stat.no/english/>. Accessed November 10, 2018.
- The Security Committee. "Ministeriöiden kyberturvallisuusstehtävät" [Ministries' Cyber Security Tasks]. February 10, 2014. <https://turvallisuuskomitea.fi/ministerioiden-kyberturvallisuustehtavat/>. Accessed November 7, 2018.
- United States Marine Corps. "Establishment of the Cyberspace 1700 Occupational Field (OCCFLD)." January 3, 2018. <http://www.marines.mil/News/Messages/Messages-Display/Article/1454562/establishment-of-the-cyber-space-1700-occupational-field-occfld/>. Accessed November 10, 2018.
- US Army Training and Doctrine Command (TRADOC). "The U.S. Army Concept for Cyberspace and Electronic Warfare Operations (2025-2040)." Pamphlet (TP) 525-8-6, January 9, 2018. <http://adminpubs.tradoc.army.mil/pamphlets.html>. Accessed October 10, 2018.
- US Cyber Command. "U.S. Cyber Command Flexes New Acquisition Muscle." October 12, 2017. <https://www.cybercom.mil/Media/News/News-Display/Article/1341294/us-cyber-command-flexes-new-acquisition-muscle/>. Accessed November 10, 2018.
- . "U.S. Cyber Command History." <https://www.cybercom.mil/About/History/>. Accessed October 5, 2018.
- US Department of Defence. "All Cyber Mission Force Teams Achieve Initial Operating Capability." October 24, 2016. <https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/>. Accessed November 10, 2018.
- . "News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium." October 4, 2018. <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/>. Accessed November 2, 2018.
- Waterman, Shaun. "Cyber Command Lacks Authorities, Capabilities, Pentagon Watchdog Says." *Cyberscoop*. September 7, 2017. <https://www.cyberscoop.com/cyber-command-lacks-authorities-capabilities-pentagon-watchdog-says/>. Accessed November 10, 2018.
- Zech, Maxime. "Dutch Cyber Defence Centre unveiled." *NLTimes.nl*. May 14, 2014. <https://nltimes.nl/2014/05/21/dutch-cyber-defense-center-unveiled/>. Accessed November 10, 2018.

Ziegler, Katja S. "The Model of a 'Parliamentary Army' Under the German Constitution." Memorandum, Minutes of Evidence, Select Committee on Constitution. House of Lords, Parliament. [https://publications.parliament.uk/pa/ld200506/ldselect/ldconst/236/5120707](https://publications.parliament.uk/pa/ld200506/ldselect/ldconst/236/5120707.htm).htm. Accessed November 10, 2018.



FOLLOW US ON:

 [FACEBOOK.COM/ICDS.TALLINN](https://facebook.com/ICDS.TALLINN)

 [TWITTER: @ICDS _ TALLINN](https://twitter.com/ICDS_TALLINN)

 [LINKEDIN.COM/COMPANY/3257237](https://linkedin.com/company/3257237)

INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
63/4 NARVA RD., 10152 TALLINN, ESTONIA
INFO@ICDS.EE, WWW.ICDS.EE



ISSN 2228-0529

ISBN 978-9949-7255-7-1 (PRINT)

ISBN 978-9949-7255-8-8 (PDF)