Report

Cyber Conscription

Experience and Best Practice from Selected Countries

| Martin Hurt | Tiia Sõmer |

February 2021

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

Title: Cyber Conscription: Experience and Best Practice from Selected Countries
Authors: Hurt, Martin; Sõmer, Tiia
Publication date: February 2021
Category: Report

Cover page photo: Ardi Hallismaa/ Estonian Defence Forces

Keywords: compulsory military service; cyber conscript; cyber reservist; defence; military training

ISSN 2228-0529
ISBN 978-9949-7484-8-8 (print)
ISBN 978-9949-7484-9-5 (pdf)

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Acknowledgements

We are very grateful to all the representatives of the Royal Danish Army Joint Signal Regiment 3 CISOPS Battalion, the Estonian Defence Forces Cyber Command, the Estonian Defence League Cyber Defence Unit, the Estonian Defence Resources Agency, Tallinn University of Technology (TalTech), Defence Command Finland, the Norwegian Armed Forces Cyber Defence, the Swedish Armed Forces Headquarters, the KTH Royal Institute of Technology (Sweden) and the Armed Forces Staff of the Swiss Armed Forces, who agreed to be interviewed for this study and who were generous with their time and frank in their opinions.

While we have received much valuable help from others, the conclusions and recommendations of this study, and any errors of fact or judgement, are ours alone.

About the authors

Martin Hurt

Martin Hurt is a Research Fellow at the International Centre for Defence and Security (ICDS) in Tallinn, Estonia. His areas of research include developments in NATO and the EU, as well as national security- and defence-related topics in the Nordic-Baltic region. He has worked as Defence Counsellor at the Estonian Permanent Representation to NATO, in various positions at the Estonian Ministry of Defence, and at the Swedish Armed Forces Headquarters.

Tiia Sõmer

Tiia Sõmer is a researcher and PhD student at Tallinn University of Technology, Estonia. Her PhD research concentrates on modelling of cybercrime. Other research interests include cyberwarfare, cybersecurity workforce challenges, and cybersecurity education and training. Before an academic career, she served for over 20 years in the Estonian Defence Forces, in posts including international assignments at NATO and the EU.

Executive Summary

Cyber conscription is quite a new phenomenon and, while there are differences between the countries that make use of it, there are also similarities. This report aims to identify best practices, exploring how countries can make best use of conscripts and reservists with information and communications technology (ICT)-related education and/or experience, bearing in mind the limited time that is available during their service. The report examines cyber conscription in six countries: Denmark, Estonia, Finland, Norway, Sweden and Switzerland. It focuses on the selection, training and employment of cyber conscripts and reservists.

The purpose of cyber conscription varies between the nations and depends on the overall purpose of conscription itself.

In the countries analysed, the number of volunteers applying for cyber conscription today exceeds the military's needs, meaning there is no immediate need to increase the attractiveness of cyber conscription. This may change, however, since several nations plan to increase the annual number of cyber conscripts to be called up.

All the countries have medical and physical requirements that conscripts of all types must fulfil. In general, these requirements apply also for cyber conscripts, with a small number of exceptions possible. In most countries the conscripts are also subject to a specific ICT-related test.

Cyber conscripts in the studied countries are selected first and foremost based on personal will and motivation, education and experience. Most cyber conscripts have IT-related educational or professional backgrounds. Few have been called up directly from high school without any IT-related education.

The interviews confirmed that cyber conscripts receive basic military training that mostly follows a uniform pattern common to all conscripts. Only after completing basic military training are cyber conscripts subjected to more specific training, including on cyberspace operations.

The interviews indicated that a dedicated reserve organisation that could draw upon citizens who have completed cyber conscription is still not fully developed in some of the studied nations that have this ambition.

Several of the studied countries' armed forces cooperate with universities and have either developed or are planning to launch partnerships with the private sector. Some provide their cyber conscripts with training that gives them a specialist certificate or university credit points.

We recommend that military authorities:

- improve their communication in order to better manage the expectations of conscripts because of the potential for misunderstandings related to the very different aspects that are linked with the term "cyber conscription"
- ensure that cyber conscription is a win-win deal from which both the armed forces and the individual conscripts clearly benefit
- develop cognitive tests that are suited for larger numbers of future cyber conscripts
- consider partnering with academia and the private sector to exploit the potential for effective specialised training as well as more efficient use of resources.

List of Abbreviations

C2	Command and control
CDIS	Centre for Cyber Defense and Information Security (KTH, Sweden)
CDU	Cyber Defence Unit
CFCS	Centre for Cyber Security (Denmark)
CIRC	Computer Incident Response Capability
CISOPS	Communication Information System Operations
CMS	Compulsory military service
CNO	Computer network operation
ECTS	European Credit Transfer and Accumulation System
EDF	Estonian Defence Forces
EDL	Estonian Defence League
EHIS	Estonian Educational Information System
FDFC5A	Finnish Defence Forces C5 Agency
ICT	Information and communications technology
ISR	Intelligence, surveillance and reconnaissance
IT	Information technology
KTH	Kungliga Tekniska Högskolan (Royal Institute of Technology, Sweden)
NCO	Non-commissioned officer
Stratcom	Strategic communications
TalTech	Tallinn University of Technology
VET	Vocational Education and Training

Introduction

Cyber defence and conscription have in recent years gained more importance and visibility. There are obviously several reasons for this, but two important developments can be distinguished: the recognition of cyber as a domain of operations comparable to more traditional ones and the deteriorating security environment that involves not only the Euro-Atlantic area but also increasing tensions between China and the West.

In July 2016 at the Warsaw Summit, NATO recognised cyberspace as a domain of operations in which the Alliance must defend itself as effectively as it does in the air, on land and at sea.[1] In addition, a number of nations, including the United States, Germany, the Netherlands and Estonia, have established a separate cyber command alongside traditional army, navy and air force commands or headquarters.[2] This underlines the importance of cyber capabilities, both defensive and offensive.

An increasing number of nations relying on conscription intend or have already started to train conscripts for a role in cyber defence

Following Russia's occupation and illegal annexation of Crimea in 2014, a number of European countries have reintroduced conscription as a means of staffing their armed forces. The evolving security environment and cyber threats, linked to digitalisation of interactions and services, gives rise to new needs of society in general and armed forces in particular. An increasing number of nations relying on conscription intend or have already started to train conscripts for a role in cyber defence. Their exact roles and responsibilities may vary and the term "cyber conscription" is therefore rather broad and covers everything from raising awareness of cyber threats among conscripts to assigning them an active role in safeguarding military and/or civilian networks. How successful are governments in harnessing the ICT-related skills of conscripts and reservists for national defence?

This report aims to identify best practices by exploring how countries can make best use of conscripts with ICT-related education and/or experience, bearing in mind the limited time that is available during their service.

The report looks at various examples of how nations use conscripts for cyber defence. It focuses on the selection, training and employment of conscripts and reservists while paying less attention to their specific tasks for security reasons. The study was conducted based on information from six nations: Denmark, Estonia, Finland, Norway, Sweden and Switzerland.

Cyber conscription is quite a new form of conscription in all countries and, while there were differences between them, there are also similarities. Cyber conscription has been conducted for a short period of time in all the countries studied, so it is too early to draw far-reaching conclusions. The aim of this report is to provide a general overview of cyber conscription as conducted in the countries studied.

The work is divided into five parts. Part 1 provides background to why conscription and cyberspace operations are relevant and gives definitions. Part 2 explains the purpose of cyber conscription in the studied countries. Part 3 explains the career management of cyber conscripts and cyber reservists by describing how cyber conscripts are recruited, selected, trained and employed. Part 4 describes examples of cooperation between the armed forces and educational institutions. Part 5 looks at the benefits, risks and challenges of cyber conscription.

[1] "Cyber defence," Topics, North Atlantic Treaty Organisation, last modified 25 September 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[2] Piret Pernik, *Preparing for Cyber Conflict: Case Studies of Cyber Command* (Tallinn: International Centre for Defence and Security, 2018), 1, http://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

1. Background, Methodology and Definitions

1.1. Background

1.1.1. Conscription

Conscription, also called the draft, is often defined as compulsory enrolment for service in a country's armed forces and it has existed as both universal and selective service.[3] Since it is often perceived as negative and linked with the notion of a mass army, some countries prefer to use the term "compulsory military service" (CMS).

Nations use conscription for different purposes and in different forms. Some nations have relatively small populations compared to the size of their territories and CMS has historically been used to increase the numerical size of the forces, accepting an offset in terms of quality in comparison with all-volunteer forces. The armed forces of Estonia, Finland and Switzerland are largely made up of mobilisable reserves maintained through a significant annual intake of youngsters who undergo CMS. Denmark has focused more on exploiting conscription as a base for recruitment of volunteers although in recent years the Danish authorities have started to emphasise the need to be able to mobilise reservists who have undergone basic military training.[4] Norway and Sweden have hybrid systems consisting of both mobilisable reserves and all-volunteers.

The current duration of conscript training and the number of citizens called up for conscription is set out in Table 1.

Whether the main reason for conscription is to persuade youngsters to join the armed forces as professionals or to prepare them to fill reserve positions, it is easy to agree with the statement from a report recently submitted to the Norwegian Ministry of Defence: conscription and CMS offer the armed forces opportunities that the private sector can only dream of.[5]

The main reason for conscription is to persuade youngsters to join the armed forces as professionals or to prepare them to fill reserve positions

A more detailed description of conscription in the analysed countries is given in Annex A.

1.1.2. Cyberspace operations

Cyberspace is now widely recognised as an essential element of national security. As a consequence, many nations are developing the role the military plays as an instrument of national defence.[6] Cyberspace operations can be defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".

	Denmark	Estonia	Finland	Norway	Sweden	Switzerland
Duration (months)	4–12	8–11	5.5–11.5	12–16	6–15	4.5
Conscripts trained per year	4,200–4,700	3,200–4,000	20,000	8,000	5,000	20,000

Table 1. Conscript training by country

[3] Britannica Online Encyclopaedia, "Conscription," https://www.britannica.com/topic/conscription.

[4] Forsvarsministeriet (Ministry of Defence) (Denmark), "Defence Agreement 2018–2023," https://fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2018-2023-pdfa-2018.pdf.

[5] Berit Svendsen et al., *Økt evne til å kombinere menneske og teknologi. Veier mot et høyteknologisk forsvar* [Increased Ability to Combine Humans and Technology. Roads to a High-tech Defence] (Oslo: Svendsen-utvalget, 2020), 87, https://www.regjeringen.no/contentassets/374492dfae2f41a18f9b01e8678b468a/svendsen-utvalget--okt-evne-til-a-kombinere-menneske-og-teknologi.pdf.

[6] Brad Bigelow, "What are Military Cyberspace Operations Other Than War?," in *2019 11th International Conference on Cyber Conflict: Silent Battle,* ed. T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga and G. Visky, (Tallinn: NATO CCD COE Publications, 2019), https://ccdcoe.org/uploads/2019/06/Art_10_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf.

They may be categorised as:

1. defensive cyberspace operations
2. intelligence, surveillance and reconnaissance (ISR) cyberspace operations
3. offensive cyberspace operations.[7]

The armed forces of the studied countries are responsible first and foremost for protecting their own networks but, in addition, some also fulfil tasks in the protection of other organisations

The armed forces of the studied countries are responsible first and foremost for protecting their own networks but, in addition, some also fulfil tasks in the protection of other organisations. As a consequence, in some nations cyber conscripts are also trained to meet the needs of stakeholders other than the armed forces.

In Estonia, a Cyber Command has been set up with the aim of carrying out cyber and information operations in cyberspace and the information sphere.[8] Its mission is to defend the information systems of the Estonian Defence Forces (EDF) and of its allies while maintaining readiness to conduct active cyber defence operations.[9]

The Finnish Defence Forces are developing the capability to maintain cyber situational awareness, for planning and implementing cyber operations, and for protecting and monitoring their systems in the cyber domain.[10] The Norwegian Armed Forces Cyber Defence branch develops, runs and protects the military communications systems and digital infrastructure.[11] From 2021, the Norwegian Armed Forces will monitor networks of the whole defence sector.

The Swedish Armed Forces monitor and analyse network traffic continuously and have the capability to carry out any type of computer network operation (CNO), including defensive and offensive actions.[12]

In Switzerland, the Federal Department of Defence, Civil Protection and Sport has sufficient qualitative and quantitative competences and capacities to disrupt, prevent or slow down attacks on critical infrastructure where necessary. The Armed Forces play a crucial role as a strategic reserve for the subsidiary support of civilian administrative units and in the event of mobilisation. The Armed Forces must therefore be able to guarantee operational readiness across all situations in the area of cyber defence, including active measures to identify threats and attackers and to disrupt and suppress attacks.[13]

1.2. Methodology

The work conducted relies on qualitative data sources: interviews, observations and articles, and public documents. The interviews were undertaken in late 2019 and early 2020 with key individuals involved in cyber defence or training of cyber conscripts. Our interviewees included personnel from and representatives of the Royal Danish Army Joint Signal Regiment 3 CISOPS Battalion, the EDF Cyber Command, the Estonian Defence League Cyber Defence Unit, the Estonian Defence Resources Agency responsible for recruitment, Tallinn University of Technology (TalTech), Defence Command Finland, the Norwegian Armed Forces Cyber Defence, the Swedish Armed Forces Headquarters, the KTH Royal Institute of Technology (Sweden) and the Armed Forces Staff of the Swiss Armed Forces.

7 Pernik, *Preparing for Cyber Conflict*, 2.

8 Ministry of Defence (Estonia), "Estonian Military Defence 2026," https://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/rkak2026-a6-spreads_eng-v6.pdf.

9 Pernik, *Preparing for Cyber Conflict*, 6.

10 Prime Minister's Office (Finland), *Government's Defence Report* (Helsinki: Prime Minister's Office Publications, 7/2017), https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf.

11 "Norwegian Cyber Defence," Organisation, Norwegian Armed Forces, last modified 11 October 2020, https://www.forsvaret.no/en/organisation/norwegian-cyber-defence.

12 "Cyber Defence," Organisation, Swedish Armed Forces, last accessed 27 October 2020, https://www.forsvarsmakten.se/en/about/organisation/cyber-defence/.

13 Federal Council (Switzerland), *National Strategy for the Protection of Switzerland Against Cyber Risks (NCS) 2018–2022* (Bern: Federal IT Steering Unit, April 2018), https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.

1.3. Definitions

"Cyber conscription" is a term that has come to be used widely. However, there is no generally agreed definition. The tasks performed by cyber conscripts vary between the countries studied. Like cyberwarfare in general, the definitions, where they exist, are national and can cover a wide range of areas. There is therefore no common approach to the term. It includes technical cybersecurity and cyber defence as well as IT support, programming and development, but often also more traditional branches such as communications/signals, intelligence, and even social media. For the purpose of this paper, the terms "cyber conscription" and "cyber conscripts" are used in the same way as the countries analysed use them.

Throughout this report, the term "basic military training" is used to describe the introductory military training in fundamental skills to which all conscripts are subjected for between two and four months to enable them to function as individuals in a military organisation. All conscripts undergo basic military training before receiving specialised training, including cyber-related training.

"Cyber conscription" is a term that has come to be used widely. However, there is no generally agreed definition

For the purpose of this paper, the terms "reservists" and "reserves" are used for citizens who have finished their military training, fill positions in the armed forces reserve and can be mobilised or called up for refresher training.

"Cyber reservist" describes the status of a cyber conscript who has completed his or her military training and is assigned to the reserve.

"Refresher training" is the term for calling up reservists and updating their military knowledge during shorter periods of time, often ranging from a couple of days to several weeks depending on the country and legal specificities.

2. Purpose

In general, the purpose of cyber conscription is to increase or support cyber capabilities in a country's armed forces, ranging from IT support to cyber defence, as explained below. The specific purpose varies between the nations and depends to a certain extent on the overall purpose of conscription, as explained in subsection 1.1.

In general, the purpose of cyber conscription is to increase or support cyber capabilities in a country's armed forces, ranging from IT support to cyber defence

Denmark is trialling the training of cyber conscripts over three years from 2020 with the main purpose of recruiting professionals after they have finished their cyber training. However, no dedicated positions for personnel with cyber skills currently exist in the military organisation. The aim is to implement them in different levels in the organisation pending the outcome of the three-year testing project. Denmark was able to recruit more than 50% of the 2020 intake of cyber conscripts as professionals to the three services (army, navy and air force) after the end of their conscription period.

In the Estonian Defence Forces, cyber conscription is used in a supporting role to reinforce some of the functions fulfilled by the Cyber Command, such as IT security and IT support, programming and development, by assisting full-time military and civilian employees. This is particularly necessary when the demand for IT services increases to levels above normal, e.g. during larger exercises or operations.[14] The first conscripts focusing on IT-related tasks were called up in 2014 when a pilot project was launched. Due to the modernisation and development of EDF IT systems, there was a need for additional personnel to conduct various tasks. As the EDF

[14] Linda-Liis Laikoja, "'Kübersõdur' on sõna, mis kõlab nagu terminaatorlik tegelane kuskilt ulmefilmist, kuid mille taga tegelikult peitub meie riigi turvalisus" ['Cyber soldier' is a word that sounds like a Terminator-like character from a science-fiction movie while in fact protecting our state], *DigiPRO*, 17 December 2020, https://digipro.geenius.ee/eksklusiiv/paev-kubersoduri-elus-on-nagu-startupis-tootamine/.

is an organisation that uses civilian resources and capabilities extensively, it was suggested that the IT knowledge and experience of conscripts should be used. Initially the number of conscripts was relatively small (a squad-size unit) and they were used as IT support personnel, but later those with more experience and knowledge were given tasks in programming and development.

Before cyber conscription was explicitly introduced in Estonia, conscripts served in various ICT-related positions. These positive experiences gave reason to introduce cyber conscription and this has been running for a number of years. All conscripts who undertake their CMS in the Cyber Command are currently formally regarded as cyber conscripts. Informally and in a narrower sense, cyber conscripts are those who work in IT-related areas in three main roles: IT development, IT support and IT security.

In Finland, cyber conscripts are male, or voluntary female, citizens who undergo CMS and who have voluntarily applied, passed a specific cyber test and been selected to serve in the Finnish Defence Forces C5 Agency (FDFC5A). Typically, they have relevant education or special interests and knowledge in the subject. Conscripts who are trained to serve on an ICT helpdesk or with combat cameras are not considered cyber conscripts as they are not required to pass the cyber test that is mandatory for cyber conscripts.

The Finnish Defence Forces have a well-developed reserve-based wartime organisation that requires a steady inflow of new personnel consisting of trained conscripts. Finland has run cyber conscription since 2015 and appears to have the greatest amount of experience of the countries studied. The annual intake of cyber conscripts is between two and 20; there is no quota. The skills of the individual conscripts are considered the most important factor, so it takes time to fill all reserve positions.

In Norway, cyber conscripts have a supporting role and help to monitor armed forces networks. The Norwegian Armed Forces Cyber Defence, which runs, secures and protects the Armed Forces' communications systems and digital infrastructure, has only 11% conscripted personnel, primarily related to communications and guard duties.[15] Since the Armed Forces will monitor the networks of the entire defence sector from 2021, the size of the cyber conscript unit will increase. Cyber conscription is also important because it forms a base from which professionals can be recruited.

The Swedish Armed Forces' training of cyber conscripts is primarily aimed at addressing the requirements of the Armed Forces but also to meet the needs of other defence organisations, including the National Defence Radio Establishment, the Swedish Defence Materiel Administration and the Intelligence and Security Service, law enforcement and rescue organisations, including the Swedish Civil Contingencies Agency, and the country's defence industry.[16]

In Switzerland, the main purpose of training cyber conscripts corresponds with the overall principle of the Swiss Armed Forces: to train personnel for the militia system. Cyber conscripts support the professional cyber specialist teams of the Swiss Armed Forces Command Support Organisation.

3. Career Management of Cyber Conscripts

This chapter explains how cyber conscripts' careers are managed, describing how they are recruited, selected, trained and employed during their CMS (service) and later (reserve). It is a summary of all findings. More detailed descriptions by country are available in Annex B.

In all countries studied, the overall career management of cyber conscripts follows a pattern illustrated by the following chart.

[15] Norwegian Armed Forces, "Norwegian Cyber Defence"; and Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 24.

[16] The National Defence Radio Establishment is the Swedish national authority for signals intelligence. The Swedish Defence Materiel Administration procures equipment and services for the Swedish Armed Forces. The Intelligence and Security Service collects and processes information on global political developments and external threats to Sweden and Swedish interests and prepares and protects the Armed Forces from security threats. The Swedish Civil Contingencies Agency (MSB) is responsible for helping society prepare for major accidents, crises and the consequences of war.

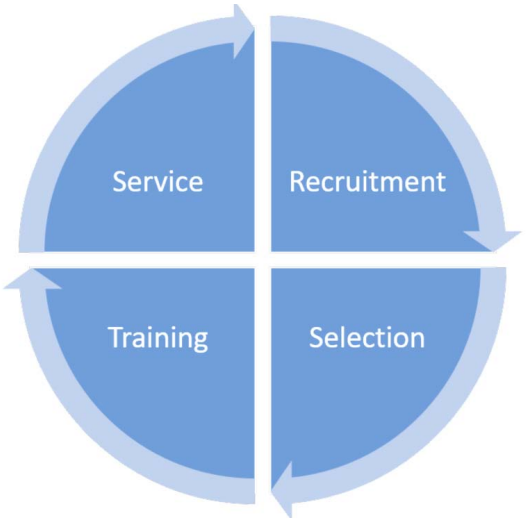

Chart 1. Career management of cyber conscripts

First, cyber conscripts are recruited together with other conscripts who will be later allocated to various units and functions within the armed forces. From this overall pool, some will be selected to become cyber conscripts based on separate criteria. These will undergo different training, after which some will also practice their skills by serving in positions. From these trained conscripts, all six countries try to recruit full-time employees. In addition, some nations also have a well-developed reserve organisation similar to other traditional branches, while other countries have a more general pool of reserves.

3.1. Recruitment

This subsection explains how the authorities identify the youngsters who are called up for CMS, regardless of what position they will serve in. It will also describe examples of how armed forces approach and attract potential cyber conscripts in order to make them aware of the possibility of serving as a cyber conscript.

In all the countries analysed, the number of volunteers applying for cyber conscription currently exceeds the military's requirements

In all the countries analysed, the number of volunteers applying for cyber conscription currently exceeds the military's requirements, so there is no immediate need to increase attractiveness of cyber-defence training for conscripts.

All countries have their own specific medical and physical requirements that conscripts must fulfil. In general, such requirements are the same for cyber conscripts, with a small number of exceptions possible. The aim of conscription is to prepare new recruits for their military tasks; they are given basic military training followed by training according to their specialisation (infantry, artillery, air defence, etc.). Cyber conscription is different as, due to its nature, cyber conscripts should ideally possess theoretical ICT-related education, either vocational education and training (VET) or a pre-university senior high school or by having started their studies at a university, or gained practical experience in the field. It would not be feasible to teach conscripts everything from scratch during a short period of CMS, as is possible in more traditional military specialisations.

Cyber conscripts in the studied countries are selected first and foremost based on personal will and motivation and previous ICT experience

3.2. Selection

This subsection describes how the most suitable individuals are selected for cyber conscript training from among other conscripts. In Denmark and Sweden, this selection process starts before the individuals are called up for CMS. In Finland and Switzerland, the cyber conscripts are selected among youngsters who have already been called up and are undergoing basic military training. Estonia employs a hybrid version combining elements of both approaches.

Children today start computer and cyber security education early. In most countries the number of applicants for cyber conscription exceeds the number of positions available, as more and more young people are educated or simply very knowledgeable about cyber security. The area is interesting to them and the armed forces therefore face the challenge of how to select the best people for cyber conscription. Cyber conscripts need to be qualified for the job, but also very motivated.

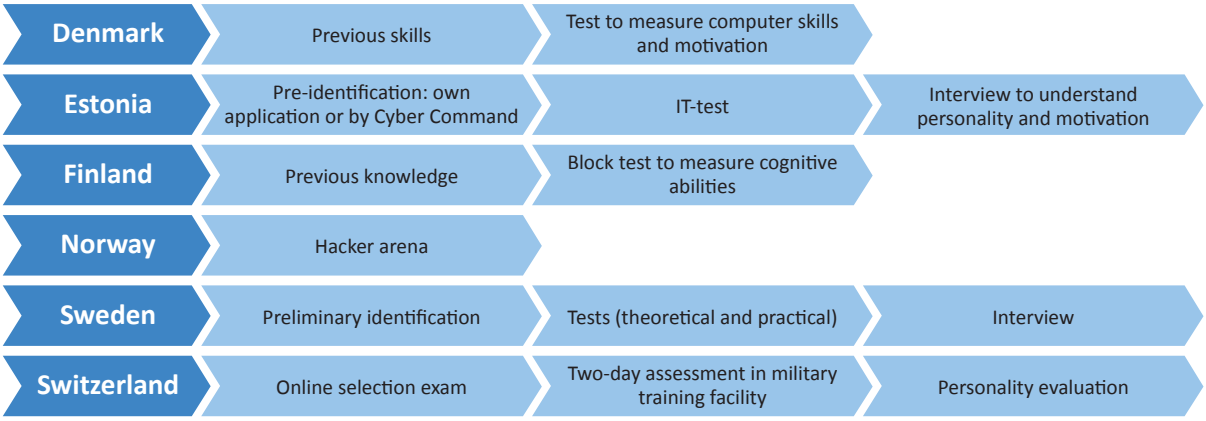

Chart 2. Selection of cyber conscripts

Each country has its own rules, regulations and procedures for this.[17] In general, cyber conscripts in the studied countries are selected first and foremost based on personal will and motivation and previous ICT experience. In most countries the conscripts are also subject to a specific ICT-related test.

The method of selecting cyber conscripts in the six countries is illustrated in Chart 2.

This chart does not aim to show an exhaustive list of activities forming part of the selection process, but it indicates the different steps that are used in the analysed countries.

Cyber conscripts receive basic military training mostly following a uniform pattern common to all conscripts. Only after completing basic military training are the cyber conscripts subjected to more specific training

3.3. Training

The interviews confirmed that cyber conscripts receive basic military training mostly following a uniform pattern common to all conscripts. Only after completing basic military training are the cyber conscripts subjected to more specific training, including on cyberspace operations. Some of the training is provided by civilian teachers, from either vocational schools or universities, and sometimes as a result of formal cooperation agreements between the armed forces and the particular vocational school or university.

Most interviewees stressed that cyber conscripts are treated more as individuals since they have to be very skilled and to function as members of small teams, unlike traditional soldiers trained to serve in larger units such as battalions. Some claimed that cyber conscripts differ from conscripts serving in more traditional roles. In Sweden and Switzerland, cyber-specific training enables conscripts to earn university credit points that will be useful for later study. Military cyber training is considered an additional qualification when applying for a job after completing cyber conscript service.

3.4. Service

After completing their cyber-specific training, cyber conscripts are used in different ways. In some countries most of the cyber conscript period is devoted to training, thus leaving little or no time for practising the learned skills by carrying out operational tasks. In such cases, on-the-job training is the closest they get to service. In other nations, cyber conscripts who have completed their specialised training play a supporting role by assisting full-time personnel in monitoring networks, participating in development or maintaining IT equipment.

[17] Tiia Sõmer et al., "Developing Military Cyber Workforce in a Conscript Armed Forces: Recruitment, Challenges and Options," in *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019)*, ed. Noelle van der Waag-Cowling and Louise Leenen (Reading, UK: Academic Conference and Publishing International, 2019), 413–421.

3.5. Reserve

The interviews indicated that the cyber reserve organisations involving cyber conscripts who have finished their training are still not fully developed in most of the countries under review. The main exceptions appear to be Finland, which has chosen to invest in quality rather than quantity when designing its cyber reserve organisation, and Estonia. Countries benefit from the work experience of cyber reservists who have developed their professional skills after finishing conscript training. Denmark does not appear to aim to develop a cyber reserve organisation.

4. Cooperation with Educational Institutions and Industry

In several of the studied countries, armed forces cooperate with universities and either have developed or are planning to launch partnerships with both academia and industry. High schools are not specifically targeted, and in some countries this is prohibited.

Danish Defence cooperates with a university that provides some of the training to cyber conscripts to ensure that they have the latest standards when it comes to IT and cyber knowledge. Other civilian institutions also provide some of the education.

In several of the studied countries, armed forces cooperate with universities and either have developed or are planning to launch partnerships with both academia and industry

In Estonia, national defence is a voluntary course in the secondary school curriculum, in which students are briefed about national defence, including but not limited to the role of conscription. The aim of national defence teaching is not military-specific learning, but "good citizenship" development in general. National defence is an elective course for upper secondary school students, lasting 70 hours.[18] Different possibilities for service in the defence forces are explained, including active duty after conscription. Often these classes are delivered by EDF personnel. In recent years and as part of the national defence course, Cyber Command personnel have started to visit high schools, vocational schools and universities to introduce cyber conscription.

The Cyber Command intends that cyber conscript training and service should count towards university studies by earning academic credit points. This is currently handled on a case-by-case basis, according to need. Also, the Defence Forces and the Kehtna Vocational Education Centre signed an agreement in late 2020 that allows students of the school's IT specialty to complete an internship during cyber conscript service starting in 2022 but this still requires formal blessing from the Ministry of Education and Research and the Ministry of Defence. In order to formalise the arrangements, a specific agreement between both ministries is required; discussions are ongoing.

Young talent can also be identified from other activities. In 2019 Estonia introduced a dedicated voluntary cybersecurity course in secondary schools, which teaches both technical and non-technical aspects of the subject. In addition to the national defence curriculum and the voluntary cybersecurity course, one school (Põltsamaa Secondary School) has introduced an in-depth IT and cyber defence specialisation to its students.[19] Outside the national school curriculum, additional activities are offered by schools, various organisations and the private sector. The Ministry of Defence also sponsors cybersecurity competitions, which has identified many young talents who have later joined cyber conscription.

In Finland, high schools are "targeted" with general defence-related education. No high

[18] Vabariigi Valitsus (Government of the Republic) (Estonia), "Gümnaasiumi riiklik õppekava 2011" [State Curriculum for Secondary Schools 2011], *Riigi Teataja* (Estonian State Gazette), RT I, 14 January 2011, 2, https://www.riigiteataja.ee/akt/128072020013?leiaKehtiv.

[19] "Infotehnoloogia (IT)- ja küberkaitse õppesuund" [Information Technology (IT) and cyber defence specialisation], Põltsamaa Ühisgümnaasium (Põltsamaa Secondary School), last modified 17 March 2020, https://www.poltsamaa.edu.ee/en/node/468.

schools offer programmes on cybersecurity, focusing more generally on sports or natural sciences. Universities in Finland play no role in training conscripts since the Finnish Defence Forces have the biggest training organisations for cyber defence.

Training in theory for cyber conscripts is constrained by the limited time available and much is on-the-job training. It is therefore important that selected conscripts already possess cybersecurity skills. The Finnish Defence Forces cooperate more frequently with private companies than with universities in order to learn from their experience and the same applies for learning from the experience of individual reservists.

In Sweden, conscripts who pass the theoretical block offered by KTH will receive about 30 credit points, which is a good reason for serving as a cyber conscript. The Swedish Armed Forces seek to launch partnerships both with academia (e.g. with KTH) and with the private sector aimed at maintaining its skills and competences on cybersecurity and cyber defence. As in Finland, the Armed Forces are not allowed to promote themselves at Swedish secondary schools.

The Swiss Armed Forces also do not cooperate with secondary schools on this subject for legal reasons. They do, however, cooperate with several universities in Switzerland. The completion of the military cyber defence course for conscripts is credited by the European Credit Transfer and Accumulation System (ECTS) towards Bachelor's degrees at several universities and schools of applied sciences. Academics and university employees (professors, Ph.D students) are also invited to lecture on the cyber defence course.

The Swiss Armed Forces reserve system provides good opportunities to be successful in the cyber domain since it exploits the knowledge and skills of citizens. Participants in the cyber defence course are also able to complete an internship outside the Armed Forces during their training. The Swiss Armed Forces cooperate with civilian authorities (e.g. the police) and operators of critical infrastructure (e.g. telecommunications and energy). The external internship is part of the practical training during basic military training and lasts eight to ten weeks. Cyber conscripts can also participate in exercises and training abroad. Some conscripts may also be offered the option to register for NATO or civilian cyber defence courses.

5. Benefits, Risks and Challenges

The interviews suggested that cyber conscription offers benefits as well as risks and challenges that need to be mitigated.

5.1. Benefits

Cyber conscription provides many opportunities:

- recruiting skilled people to the armed forces
- providing armed forces with up-to-date innovative knowledge from civil society
- providing young people with work experience that can be useful in their careers
- raising awareness of cyber issues in wider society.

One of the more obvious benefits of cyber conscription is that it brings to the armed forces qualified citizens with up-to-date knowledge on IT and cybersecurity who would otherwise probably not have served in the military

One of the more obvious benefits of cyber conscription is that it brings to the armed forces qualified citizens with up-to-date knowledge on IT and cybersecurity who would otherwise probably not have served in the military. While most conscripts leave the military after the training period, some are offered full-time service. A report of April 2020 concluded that the primary benefit of cyber conscripts and reservists resides in the fact that they help the armed forces to conduct relevant tasks and thus close the workforce gap in the field of cybersecurity. All armed forces have difficulty hiring permanent personnel, but reserve positions seem to be valued more

highly and filled more easily.[20] As stated in a report recently submitted to the Norwegian Ministry of Defence, conscription and CMS offer the armed forces opportunities that the private sector can only dream of.[21] According to one interviewee who contributed to the ICDS report, the salary levels of the Finnish Defence Forces mainly attract two categories of people: young university graduates and more experienced people in their 50s who value interesting tasks more than money.

One clear benefit for both the armed forces and conscripts is the potential for future full-time service.

To the individual, cyber conscription offers the possibility to increase cybersecurity- and cyber defence-related skills through training and practice. Another clear benefit for youngsters is receiving ECTS points or other certificates of training after completing service. Interviewees put forward different aspects. In Sweden, the 30 credit points that conscripts receive after completing their CMS are a good motivator. Finns receive a certificate that proves they have been cyber conscripts, which is beneficial in their future studies or work careers.

In addition, the word "cyber" attracts young people, which is why it is more effective to talk about "cyber soldiers" than "IT soldiers". The armed forces exploit this phenomenon and highlight the benefits of cyber conscription for future career opportunities as cyber-defence specialists or for academic studies.

The Swiss Armed Forces draw on the knowledge of the country's citizens. Due to the reserve system, members of the army can incorporate the skills they acquire in their civilian profession into the armed forces. From the conscript's point of view, this offers the opportunity to prepare for a civilian cybersecurity exam during military service. After passing a three-day exam, the conscript will graduate as a Cyber Security Specialist with a Swiss Federal Specialist Certificate. Due to the increasing shortage of ICT and cyber experts in the economy, these specialists are very attractive for Swiss companies.

The approach of Swedish authorities – that the armed forces train cyber conscripts primarily to meet their own requirements but also to meet the needs of other organisations involved in national defence as well as law enforcement, rescue organisations and the defence industry – merits consideration by decision-makers in other nations. To what extent should the annual number of trained cyber conscripts depend on the requirements of the military, and how far can the government afford to increase supply beyond the needs of the military and other organisations vital for defence and security in order to create a positive spillover effect that will benefit society at large, including the private sector? This is a relevant question not least because critical national infrastructure essential for the functioning of a society and an economy is often owned and operated by private companies.

One risk is the possibility that the cyber training that will be offered by the military differs from the youngsters' expectations, especially operational tasks. This risk implies that it is important to manage expectations and that the information provided before call-up is precise and thus leaves less room for disappointment

5.2. Risks and Challenges

While cyber conscription offers obvious benefits both to the armed forces and to conscripts, there are also risks and challenges. Conscripts are young people and their social maturity might not be adequate to carry the responsibility of a cyber conscript.[22] During their service they may have access to sensitive or classified information, or to critical information systems. The most obvious risks

[20] Marie Baezner, "Study on the use of reserve forces in military cybersecurity: A comparative study of selected countries," Center for Security Studies (CSS), ETH Zürich, 35, https://doi.org/10.3929/ethz-b-000413590.

[21] Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 87.

[22] Sõmer et al., "Developing Military Cyber Workforce in a Conscript Armed Forces."

are information leaks or the use of tools and skills for unlawful purposes after conscription, to a certain degree comparable with the potential misuse of knowledge of how to handle weapons.

Another risk is that it may become difficult in future to recruit cyber conscripts if they are not motivated to undergo basic military training. This risk is obviously more relevant in those countries where cyber conscripts are recruited among youngsters who have the option not to serve at all. Today most cyber conscripts volunteer for their cyber service. This risk is less likely to materialise in Finland, for example, where cyber conscripts are selected from among those who already have started their CMS.

One risk that has been highlighted is the possibility that the cyber training that will be offered by the military differs from the youngsters' expectations, especially operational tasks and perhaps even hacking. This risk implies that it is important to manage expectations and that the information provided before call-up is precise and thus leaves less room for disappointment.
Another challenge is how to avoid the potential perception that conscripts (or reservists) are used as "free labour", especially in cases where the employment of cyber conscripts exceeds the amount of training they receive. This can be mitigated as long as the armed forces are able to offer a win-win deal for both parties by ensuring that every person (conscript or reservist) will gain knowledge. A second risk is related to enlarging the pool of reservists: the smart use of the increasing number of reservists.

There are opportunities to be exploited by widening the scope of recruitment of conscripts beyond those who fulfil all medical and other requirements. This may not seem urgent today since there is no lack of volunteers, but the situation may change in the future.
Several countries have declared their intention to increase the number of cyber conscripts taken on each year. Consequently, a big risk is a lowering of quality standards due to the increase in quantity.

Conclusions and Recommendations

This report has examined cyber conscription in six countries to identify best practices and has focused on the selection, training and employment of cyber conscripts and reservists. Based on the interviews, documents and articles, it is possible to draw a number of conclusions.

1. The purpose of cyber conscription varies between the countries analysed and depends on the overall purpose of conscription. In some countries, cyber conscription is not only intended to increase the cyber capabilities of the armed forces but also to support other organisations involved in national defence.

2. There is no generally agreed definition of the term "cyber conscription". It may include cybersecurity and cyber defence more narrowly but also IT support, programming and development, as well as more traditional branches such as communications/signals, intelligence and strategic communications (stratcom).

3. Among the countries surveyed, the number of volunteers applying for cyber conscription today exceeds the military's requirements, so there is no immediate need to increase the attractiveness of cyber conscription.

4. All six countries have medical and physical requirements that all conscripts must fulfil. In general, these apply also for cyber conscripts, with a small number of exceptions.

5. Cyber conscripts in the studied countries are selected first and foremost based on personal will and motivation, education and experience. Most cyber conscripts have IT-related educational or professional backgrounds. Few have been called up directly from high school without any IT-related education.

6. In most countries the conscripts are also subject to a specific ICT test.

7. The interviews confirmed that cyber conscripts receive basic military training that mostly follows a uniform pattern common to all conscripts. Only after completing the basic military training are the cyber conscripts subjected to more specific training, including on cyberspace operations.

8. The length of cyber-specific training varies between the countries. In some, cyber conscripts undergo a bespoke curriculum that is implemented in cooperation with universities and/or external individual lecturers, while in others the amount of cyber-specific training is more modest.

9. Several of the studied countries' armed forces have either developed or are planning to launch partnerships with the private sector.

10. Some armed forces provide their cyber conscripts with training that gives them a specialist certificate or academic credit points.

11. The interviews indicated that a dedicated reserve organisation that could draw upon citizens who have completed cyber conscription is still not fully developed in some of the studied nations that have this ambition.

12. Several countries plan to increase the number of cyber conscripts who will be called up each year. In addition, the armed forces are still considering how to design cyber conscription in order to maximise the value it adds.

The use of conscripts for relatively complicated cybersecurity- and cyber defence-related tasks requires extensive training. Some armed forces provide training with in-house resources, while others involve universities and the private sector. Decisions on whether a lot of resources should be invested in providing conscripts with high-level education depend on the purpose of conscription, as described in Section 2, and the differing purposes of cyber conscription. Countries that mainly call up cyber conscripts in order to create a pool from which to recruit full-time military and civilian personnel may prefer to spend less resources on training them. Those that wish to educate citizens beyond the peacetime requirements of the armed forces to fulfil the needs of a reserve organisation or other actors in the public and private sector that are vital for national defence may deem that training conscripts is the right way forward.

We recommend that military authorities improve their communication to better manage the expectations of conscripts; ensure that cyber conscription is a win-win deal; develop cognitive tests and; consider partnering with academia and the private sector

The following recommendations may be useful for countries that train or consider starting training conscripts for cyber defence. Based on the best practice identified in this report, we recommend that military authorities:

- **Improve their communication** in order to better manage the expectations of conscripts because of the potential for misunderstandings related to the very different aspects linked to the term "cyber conscription". Although there is no immediate need to increase the attractiveness of cyber conscription as there are enough volunteers, armed forces should consider devoting more effort to explaining the content of cyber conscription and communicate this effectively to youngsters in order to manage their expectations and avoid misunderstanding.

- **Ensure that cyber conscription is a win-win deal** from which both the armed forces and the individual conscripts clearly benefit. While there is no shortage of volunteers to join cyber conscription today, the armed forces should strive to retain its current positive image by providing a challenging and interesting environment in which young people gain knowledge and develop their skillsets. In the case of cyber conscription, a lot of information travels by word of mouth and a single negative experience could ruin years of hard work. This would mitigate the potential

perception that conscripts and reservists are exploited as "free labour".

- **Develop cognitive tests** that are suited to larger numbers of future cyber conscripts. All six countries studied currently use selection procedures to identify people with suitable mindsets and skillsets for cyber conscription. While the selection procedures work well and often are individually tailored, they appear to be rather resource-heavy bearing in mind that all countries assume the number of cyber conscripts will increase in the future. This can be mitigated by developing specific cognitive tests to measure mindset, skillset, stress management, leadership skills and personal qualities. The flexible and individual approach towards recruiting used by most countries today should be retained to the extent possible.

- **Consider partnering with academia and the private sector** to exploit the potential for effective specialised training as well as more efficient use of resources.

Annex A. Conscription in General

Cyber conscription should be seen in a broader context of conscription as a means to recruit personnel to the armed forces of the studied countries.

In Denmark, conscription comprises a relatively insignificant number of young males. Overall, the length of training depends on the unit and the position and varies between four and 12 months.[23] Until recently, Denmark's basic, four-month training period was intended above all to encourage conscripts to join as professionals. The latest Defence Agreement, covering the period 2018 to 2023, increases the number of conscripts trained each year by 500 (from 4,200 to 4,700) and extends training for some of them from the current four months to eight.[24]

In Estonia, a significant part of the EDF consists of a reserve component that is maintained by an annual intake of conscripts who are trained and later assigned to a reserve unit. CMS lasts eight or 11 months, depending on the assignment and the amount of training it requires. Some 3,200 conscripts are trained annually; this number will increase to 4,000 by 2026.[25]

In Finland, general conscription and training the entire able-bodied annual intake of men produce the Defence Forces' wartime organisation in a cost-effective manner.[26] More than 20,000 young male citizens undergo CMS each year.[27] Depending on the training, military service lasts 165, 255 or 347 days. Conscripts trained for rank-and-file duties serve for 165 days (five and a half months), while those trained for rank-and-file duties requiring special skills and those completing unarmed service serve for 255 days (eight and a half months). Conscripts trained to be officers or non-commissioned officers, or for the most demanding special duties in the rank-and-file, serve for 347 days (11.5 months).[28] CMS is regarded very highly and youngsters who have neither received military training nor undergone the alternative civilian training are often considered less attractive on the labour market.

In Norway, citizens have the obligation to serve a total of 575 days (19 months), divided between military training ("*Førstegangstjeneste*" in Norwegian, meaning "first-time service") with a duration of 12 or 16 months and participation in refresher exercises and service in the Norwegian Home Guard. Since 2015, both men and women must undergo CMS; the annual number of citizens to be trained is 8,000.[29] The aim is to select the most suitable and the most motivated for CMS.

In Norway, citizens have the obligation to serve a total of 575 days (19 months), divided between military training with a duration of 12 or 16 months and participation in refresher exercises and service in the Norwegian Home Guard

Due to the deteriorating security environment combined with difficulties in staffing the Swedish Armed Forces as an all-volunteer organisation, the Swedish government decided in March 2017 to reactivate conscription, this

[23] "Efter Forsvarets Dag" [After Defence Day], Forsvaret (Danish Defence), last accessed 10 November 2020, https://karriere.forsvaret.dk/varnepligt/forsvaretsdag/efter/.

[24] Piotr Szymański, "Overstretched? Denmark's security policy and armed forces in light of the new Defence Agreement," OSW Commentary no. 266, 20 April 2018, http://aei.pitt.edu/93810/1/commentary_266.pdf.

[25] Kaitseministeerium (Ministry of Defence) (Estonia), *Aruanne kaitseväekohustuse täitmisest ja kaitseväeteenistuse korraldamisest 2019. aastal* [Report on the Fulfilment of Military Service and on the Organisation of Conscription in 2019] (Tallinn: Kaitseministeerium, 2020), https://www.kra.ee/static/aruanne_kaitsevaekohustuse_taitmisest_riigis_2019.pdf; Ministry of Defence (Estonia), "Estonian Military Defence 2026."

[26] Prime Minister's Office (Finland), *Government's Defence Report*.

[27] Anti Rinne, *Hallituksen esitys eduskunnalle valtion talousarvioksi vuodelle 2020* [Government Proposal to Parliament for State Budget of 2020] (Helsinki: Edita Prima Oy, 2019), 260, https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_29+2019.pdf.

[28] "Conscription - a Finnish choice," Conscription, Finnish Defence Forces, last accessed 20 October 2020, https://puolustusvoimat.fi/en/finnish-conscription-system.

[29] "Verneplikt"[Conscription], Forsvaret (Norwegian Armed Forces), last accessed 3 November 2020, https://forsvaret.no/forstegangstjeneste/verneplikt; Store Norske Leksikon (Great Norwegian Encyclopaedia), "Verneplikt" [Conscription], https://snl.no/verneplikt.

time for both male and female citizens. There is currently a need to train 5,000 soldiers annually and this number is planned to increase to at least 8,000 by 2025 since the new wartime organisation will consist of 90,000 positions compared to the current 60,000.[30] Conscripts are currently trained for between six and 15 months.[31]

In Switzerland, conscription is used to train individuals for the armed forces, which are organised as a militia.[32] Military service of 18 weeks is compulsory for men aged 18 and over and voluntary for female citizens.[33]

[30] Regeringskansliet (Government Offices) (Sweden), "Regeringens proposition 2020/21:30. Totalförsvaret 2021–2025" [Government Bill 2020/21:30. Total Defence 2021–2025], Stockholm, 14 October 2020, https://www.regeringen.se/4a965d/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsproposition-2021-2025/totalforsvaret-2021-2025-prop.-20202130.pdf.

[31] "Grundutbildning med värnplikt" [Basic military training under conscription], Försvarsmakten (Swedish Armed Forces), last accessed 27 October 2020, https://jobb.forsvarsmakten.se/sv/ordlista/#/word/militar-grundutbildning.

[32] Federal Council (Switzerland), "Federal Constitution of the Swiss Confederation. Art. 58–59," https://www.admin.ch/opc/en/classified-compilation/19995395/index.html.

[33] "Dienstpflicht" [Obligation to serve], Schweizer Armee (Swiss Army), last accessed 30 November 2020, https://www.vtg.admin.ch/de/mein-militaerdienst/allgemeines-zum-militaerdienst/dienstpflicht.html.

Annex B. Recruitment, Selection, Training and Employment of Cyber Conscripts

This annex describes the recruitment, selection, training and employment of cyber conscripts during (service) and after (reserve) conscription, by country.

B.1. Recruitment

All Danish men living in Denmark are called up to participate in the "Defence Day" (*Forsvarets dag*) the year they turn 18. There they are informed about everyday life in the Danish Army, Navy and Air Force and the Danish Emergency Management Agency, and hear more about conscript training. Women are invited to this event, but their participation is voluntary. Attendees take a written test covering logical thinking, Danish language skills, mathematics and geometric reasoning abilities, and have their health examined by a doctor to find out if they are suitable for military service. The current proportion of volunteers is over 99%, which means that, as a rule, practically no one is forced into military service.[34]

Estonian male citizens are subject to conscription between the ages of 17 and 27. Female citizens can volunteer. First, youngsters are called up to receive information about CMS, to undergo medical examination and to present their personal preferences regarding when and where to serve.[35] University students can apply for an extension and select when to be called up during their higher education studies. In 2019 about 9,600 citizens were processed, of whom 3,870 (40%) were deemed fit for service; 59.8% were deemed to be temporarily (33.5%) or permanently (26.3%) unfit, mainly due to musculoskeletal or connective tissue diseases and psychic behavioural disorders.[36] 3,298 youngsters started their CMS, of whom 43% had volunteered.[37] An increasing number of conscripts volunteer to join the defence forces collectively, meaning that entire school classes join and serve together.[38]

Recruitment and selection of conscripts for CMS is partly based on information from the Estonian Educational Information System (EHIS), among other national databases. This system, however, does not record individual talents or skills. In addition, the current system does not reflect draftees' possession of vocational (or other) standards or certificates, their language skills or any other specific skills that could be useful in the cybersecurity field.

In Estonia, an increasing number of conscripts volunteer to join the defence forces collectively, meaning that entire school classes join and serve together

Medical requirements for Estonian cyber conscripts are the same as for any other conscripts. In specific cases and based on individual preferences, those who do not pass the medical test may still be accepted for service. In such cases, Cyber Command medical staff will examine the individual and discuss the situation with them, after which a separate decision is made. The conscript must still undergo basic military training. Conscripts who have been assigned to the Cyber Command take a simple IT test upon arrival to establish their skills. The vetting process is then initiated for those who need security clearance; the requirement varies between positions.

In Finland, all male citizens are summoned for call-up the year they turn 18. Having filled in a questionnaire in advance, their state of health is checked and their wishes concerning their conscript service are noted. On the basis of the information available, the individual's suitability and fitness for military service will be assessed and determined. The period

[34] "Forsvarets dag" [Danish Defence day], Forsvaret (Danish Defence), last accessed 10 November 2020, https://karriere.forsvaret.dk/varnepligt/forsvaretsdag/.

[35] "Arstlik komisjon" [Medical board], Kaitseressursside Amet (Defence Resources Agency) (Estonia), last modified 31 December 2020, https://kra.ee/arstlik-komisjon/.

[36] "Kõrgharidus ja ajateenistus" [Higher education and conscription], Kaitseressursside Amet (Defence Resources Agency) (Estonia), last modified 27 August 2020, https://kra.ee/ajateenistus/ajateenistusest/korgharidus-ja-ajateenistus/.

[37] Kaitseministeerium (Ministry of Defence) (Estonia), *Aruanne kaitseväekohustuse täitmisest ja kaitseväeteenistuse korraldamisest 2019. aastal.*

[38] Tiina Jaakson, "Klassikaupa ajateenistusse minek on üha populaarsem" [School classes undergoing conscription together increasingly popular], *ERR,* 13 July 2020, https://www.err.ee/1112450/klassikaupa-ajateenistusse-minek-on-uha-populaarsem.

and location of service will be assigned, or exemption from military service decided.[39] Once the individual has started his or her CMS, a "block test" is conducted. This basic test focuses on fundamentals of thinking. It measures a person's cognitive abilities, as well as emotional balance, self-confidence, leadership skills, speed of decision-making, social skills and motivation.[40] Block tests are carried out in all military units, and cyber conscripts can be selected from all such units. The results of these tests are used to determine the individual's suitability for a wide range of positions in the wartime organisation.

Every year some 60,000 Norwegian male and female citizens who are about to turn 17 are obliged to fill in an online questionnaire about their social life, health, physical condition, motivation, interests and preferences. None of these questions look at gaming, programming, technology or cybersecurity. Based on the answers, the authorities call up 19,000 people for comprehensive medical examinations, which are the next step on the way to CMS, education or a job in the Armed Forces.[41] These examinations include tests of physical fitness and intellectual performance, review of any documented diseases or disabilities, general clinical examinations and interviews, and tests of visual acuity and colour vision, and audiometry.[42] Half of those who attend comprehensive medical examinations are subsequently selected to serve in the Armed Forces.[43] Nine per cent of those who complete their CMS are later recruited by the Armed Forces.[44]

The year a Swedish citizen turns 18, he or she must submit information to the Swedish Defence Recruitment Agency on the internet based on 60 questions about the individual's health, interests and education. An assessment is made to determine whether the individual should be summoned to muster, together with some 13,000 other citizens per year. The "mustering" consists of tests, examinations, assessments and interviews, and officials determine if the individual is suited for national service with the Swedish Armed Forces.[45] A decision based on this selection process is made within four months.

In Switzerland, CMS is preceded by an "orientation day" (*Orientierungstag*), which is compulsory for all Swiss men over the age of 18. Interested women can participate voluntarily. During the orientation day, youngsters are informed about the armed forces, civil defence, the Red Cross and alternatives for non-military service. Preferences related to service time and location of training are discussed. They must submit information for a personal security check and a medical check-up, which affect the next step: recruitment (*Rekrutierung*).[46] This process lasts for two to three days, between three and 12 months before actual call-up to service. During *Rekrutierung*, the youngster will be subject to medical examination, a fitness test, a psychological evaluation and the personal security check.[47] In the course of the recruitment process, a commission of inquiry

[39] "Call-ups," Conscript Webpage, Finnish Defence Forces, last accessed 20 October 2020, https://intti.fi/en/call-ups.

[40] Tiia Korhonen, "Puolustusvoimien 'pällitestin' kysymykset huvittavat – mistä kokeessa on oikeasti kysymys?" [The questions in the "top test" of the Defence Forces are amusing - what is really the question?], *Yle*, 29 August 2017, https://yle.fi/uutiset/3-9798024; and Jarmo Huhtanen, "'Se on nyt modernimpi psykologisia käsitteitä mittaava testi' – Armeija uusii varusmiesten 'palikkatestit', nämä viisi väitettä karsiutuivat lopullisesta versiosta" ["It is now a more modern test measuring psychological concepts" – Army renews conscript "block tests", these five claims were eliminated from the final version], *Satakunnan Kansa*, 8 May 2020, https://www.satakunnankansa.fi/a/0c279474-8446-4540-9673-7d47adca85ae.

[41] "Egenerklæring" [Self-declaration], Forsvaret (Norwegian Armed Forces), last accessed 3 November 2020, https://www.forsvaret.no/egenerklaering; and Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 24.

[42] Elin Anita Fadum, Einar Kristian Borud and Leif Aage Strand, "The Norwegian Armed Forces Health Registry and use of military screening data to evaluate changes in IQ scores over time," *Revue d'Épidémiologie et de Santé Publique* (Journal of Epidemiology and Public Health), Vol. 66, Supplement 5 (2018), S343, https://www.sciencedirect.com/science/article/abs/pii/S0398762018309878.

[43] "Sesjon" [Examination], Forsvaret (Norwegian Armed Forces), last accessed 3 November 2020, https://www.forsvaret.no/sesjon.

[44] Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 26.

[45] Swedish Defence Recruitment Agency, "A duty not reserved for everyone," https://www.rekryteringsmyndigheten.se/globalassets/dokument/varnplikt/2020/191209_en_rek_trycksak_a5_aw.pdf; "Mönstringsunderlag" [Basic information for mustering], Rekryteringsmyndigheten (Swedish Defence Recruitment Agency), last modified 6 February 2021, https://www.pliktverket.se/totalforsvarsplikten/monstring-och-monstringsunderlaget/monstringsunderlaget.

[46] "Mein Orientierungstag" [My orientation day], Schweizer Armee (Swiss Army), last accessed 30 November 2020, https://www.vtg.admin.ch/de/mein-militaerdienst/stellungspflichtige/orientierungstag.html#ui-collapse-502.

[47] "Bereit für die Rekrutierung?" [Ready for recruitment?], Schweizer Armee (Swiss Army), last accessed 30 November 2020, https://www.vtg.admin.ch/de/mein-militaerdienst/stellungspflichtige/rekrutierung.html.

will decide on the individual's suitability, followed by an assignment interview with a recruiting officer for either the army or civil defence, depending on requirements.

B.2. Selection

In Denmark, would-be cyber conscripts need to meet the same medical requirements as any other conscripts. They must also have language/written competences in Danish (read, understand and write technical documents) and English (read and understand technical documents), have knowledge of installing client operating systems, have a general understanding of networks and of the structure of a computer and, last but not least, be likely to receive a security clearance at the level of Secret.[48] In addition, they must pass a test assessing computer skills and basic understanding of a computer and networks, plus a psychological conversation to ensure that they are motivated and for the right reasons. This testing takes place before the conscripts start their CMS.

Denmark has recently run a first cyber conscription intake, in which 16 out of 80 applicants were selected. Most young people today meet the requirements and criteria; the limitation is in training facilities, which allow for only 16 personnel. For the first three years it is planned to conduct intakes twice a year, in February and August. After each batch, an evaluation will take place and the training for the next batch adjusted as required. After three years the success of cyber conscription will be assessed. The Danish Ministry of Defence has indicated interest in increasing numbers.

In Estonia, cyber conscription is voluntary. If a conscript has a suitable IT background but does not wish to serve in the Cyber Command, he will not be obligated to do so. For the most part, suitable candidates are often pre-identified. Either they have contacted the Cyber Command or the Cyber Command or the Cyber Defence League has recommended the Defence Resources Agency to encourage specific individuals to apply for service as a cyber conscript based on information obtained through cooperation with secondary schools. Information about the possibility of cyber conscription travels by word of mouth among former conscripts. Upon joining the Cyber Command, a two-part selection process is initiated: test and interview. The cyber soldier selection test has been developed by the Cyber Command and includes questions about various ICT topics. After testing, the candidates are interviewed. The aim of the interview is to gain an understanding of a person's motivation, previous education (some of which may not be included in national databases), work experience and knowledge of various technologies. The position in which an individual conscript will serve is a function of the requirements of the defence forces, the person's previous knowledge, the results of the Cyber Command's IT test and the interview. There are currently sufficient volunteers from which to select. Those who have joined cyber conscription have related educational or work backgrounds. Very few come directly from high school without formal IT education or work experience. Most have either graduated from a university or have a couple of years of professional experience.[49]

Norway uses a hacker arena to promote the Armed Forces and to recruit talent to the cyber college

Cyber conscription is demanding and the Finnish Defence Forces are looking for youngsters who already have cybersecurity-related skills and competences, who have a high school diploma or occupation in cybersecurity, a general interest in cybersecurity, or who are studying cybersecurity at university. Motivation is also an important factor. All cyber conscripts are volunteers among conscripts who have started their training, and they need to pass three elements of a selection process that takes place during basic military training: a test, an interview and a security check. The test focuses on cyber and includes the ability to read code and logs to find anomalies. Medical requirements for cyber conscripts are the same as for other conscripts since they are

[48] "Cyberværnepligt" [Cyber conscription], Forsvaret (Danish Defence), last accessed 10 November 2020, https://karriere.forsvaret.dk/varnepligt/varnepligten/cybervarnepligt/.

[49] Laikoja, "'Kübersõdur' on sõna, mis kõlab nagu terminaatorlik tegelane kuskilt ulmefilmist, kuid mille taga tegelikult peitub meie riigi turvalisus."

selected among the pool of conscripts who are already undergoing basic military training.

Finnish cyber defenders promote themselves in order to increase the awareness of youngsters using four main channels or events.

1. "Disobey" is a hacker event that has been held annually since 2015.[50]
2. "Assembly" is an ICT gaming event that has been organised for many years.
3. The Finnish Defence Forces send representatives to schools to conduct follow-up education of teachers.
4. Stratcom for recruitment of full-time employees.

Norway uses a hacker arena to promote the Armed Forces and to recruit talent to the cyber college, but it is unclear how useful this has been. In 2019 the Norwegian Ministry of Defence commissioned a study to provide input on how to use relevant lessons learned from private business and other enterprises to improve the Armed Forces' ability to recruit, retain and develop competence. According to the findings published in June 2020, the military is not yet very successful in using CMS to identify talent with special skills in cybersecurity.[51]

In Sweden, youngsters who volunteer for and are deemed suitable for cyber conscription undergo an additional selection process before starting their basic military training. This additional process involves theoretical and practical tests, and interviews. A decision whether to call up an individual for cyber conscription is based on skills and knowledge as well as the individual's personality and motivation. In 2020, of the 70 conscripts who volunteered for the additional selection process, 30 were selected for cyber-defence training.[52] Every cyber conscript is subject to an eight-week vetting process with a view to issue of security clearance.

The Swiss Armed Forces recruit cyber conscripts among IT specialists who successfully complete their apprenticeship.[53] The concept of the course also allows high school graduates to attend. The Armed Forces look for candidates who have achieved a high grade in IT training, those who have a high school degree and good knowledge in IT and cyber, and "geeks" who obtained their capabilities elsewhere (e.g. self-tuition). To be accepted for the military cyber defence course, every candidate must prove his or her knowledge in a two-step selection process. Cyber conscripts are recruited from all branches of the Armed Forces a few weeks after the start of their basic military training.

The Swiss Armed Forces recruit cyber conscripts among IT specialists who successfully complete their apprenticeship

Every recruit who fulfils the requirements mentioned above is allowed to participate in the first selection exam. This 90-minute online exam tests the conscripts' knowledge of mathematics and computer science. For the second selection step, the top 50 from the first round are invited to a two-day assessment at a military training facility. During this assessment, candidates' technical abilities and knowledge in the cyber domain are examined, complemented by an intelligence test. In addition, the candidates' personality is evaluated and an extended security check carried out. Only the top 20 candidates of the second assessment are invited to attend the cyber defence course. The first group of cyber conscripts to be trained was selected among 140 applicants.[54]

[50] The 2021 event has been postponed to 2022. See "Disobey postponed to 2022," Disobey, last accessed 28 January 2021, https://disobey.fi/2021/.

[51] Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 23.

[52] Försvarsmakten (Swedish Armed Forces), "Första kullen cybersoldater redo att rycka in" [First cyber conscripts ready to be called up], 18 May 2020, https://www.forsvarsmakten.se/sv/aktuellt/2020/05/forsta-kullen-cybersoldater-redo-att-rycka-in/.

[53] Switzerland employs a unique system of apprenticeship. Pupils face an important choice at the end of their three compulsory years in lower secondary school. When moving on to upper secondary level, they can either enrol in VET or, if their marks are good enough, go to a pre-university senior high school. Most VET programmes are dual-track, combining part-time classroom instruction at a vocational school with a part-time apprenticeship at a host company, with more days of the week spent in the workplace. The system allows young people to acquire professional skills that are in demand, and paves their way into the labour market. See "Apprenticeship system," swissinfo.ch, last modified 19 February 2019, https://www.swissinfo.ch/eng/apprenticeship-system/43796482.

[54] Alexandra Aregger and Oliver Borner, "Schweizer Armee hat ihre ersten Cyber Rekruten ausgebildet" [The Swiss Army has trained its first conscripts], *Nau.ch*, 26 May 2019, https://www.nau.ch/news/videos/schweizer-armee-hat-ihre-ersten-cyber-rekruten-ausgebildet-65526664.

B.3. Training

Danish cyber conscripts serve for ten months and are subjected to basic military training for the first four months, followed by six months focused on IT and cyber-defence training, on-the-job training and cyber exercises. The purpose of this training is to demonstrate to the conscripts how the military uses cyber defence on the battlefield but individuals are not trained for specific positions. Most of the cyber-specific training takes place in classrooms. The focus is on training rather than service. During the theoretical and practical training, the conscripts learn about networks, servers, databases, Linux and so on with the goal of being able to build a small network with infrastructure and basic services. Thereafter, the cyber conscripts receive two weeks on-the-job training, for example the Centre for Cyber Security (CFCS), which is the national IT security authority whose mission is to advise the Danish public authorities and private companies that support essential services on how to prevent, counter and protect against cyber-attacks.[55]

In Denmark, the conscripts learn about networks, servers, databases, Linux etc with the goal of being able to build a small network with infrastructure and basic services. Thereafter, the cyber conscripts receive two weeks on-the-job training

Most training of Danish cyber conscripts takes place in small groups (four by four, red and blue teams), in classrooms with 24-hour access. Some of the training is provided by civilian teachers over a period of 15–16 weeks at a civilian school that focuses on practical computer skills. Significant effort is made to keep the individuals motivated. As with signals conscripts, who work at squad level, six to nine individuals who are also cyber conscripts will be trained as individuals and in small groups (four-strong teams, red and blue). There are similarities with technical positions in the signals regiment normally filled by professionals. Computer support personnel are always in demand in the regiment to build networks and so on, and they are taught how to offer services and how to harden systems and networks, including what to do in the five phases of a cyber-attack. Cyber conscripts receive ten weeks of such training while professional computer supporters receive 25 weeks. Professional computer support personnel are usually recruited after they have completed their CMS. The technical training offered by Danish Defence is the same as on the civilian market, where salaries are higher. Retention is therefore a challenge.

In Estonia, cyber conscription lasts 11 months and a number of conscripts later sign up for active duty, which indicates that cyber conscription is indeed an effective recruiting base. There are usually two intakes per year (February and June) of around 40 individuals each. Basic military training is the same as in other units (eight weeks). Cyber-related training focuses on the specifics of the systems that are used by the EDF. Since 2019, a dedicated ten-week cyber NCO specialisation course focusing on cyber and leadership skills has been run, but not all cyber conscripts are able to attend this. The cyber element of the course includes IT development processes, technologies, information systems, management of business continuity for IT services, recovery, backup, and user management. Some specific training is outsourced from the EDF, for example training to improve communication skills, including the ability to put forward ideas and proposals clearly and concisely.

All Finnish conscripts undergo basic military training that includes about eight hours of cybersecurity and cyber-defence training. After the basic three-month soldiers' training in different units, cyber conscripts are sent to the FDFC5A in Jyväskylä, about 270km north of Helsinki. There they receive military cyber education and specialist training. The FDFC5A supports Defence Command Finland with IT services including cyber defence. After receiving military cyber education and specialist training, the conscripts continue to serve either in the FDFC5A or in respective headquarters cyber

[55] Center for Cybersikkerhed (Centre for Cyber Security) (Denmark), "Nysgerrige cyberværnepligtige besøgte CFCS" [Curious cyber conscripts visited CFCS], 2 November 2020, https://cfcs.dk/da/nyheder/2020/nysgerrige-cybervarnepligtige-besogte-cfcs/.

cells. All training of cyber conscripts takes place in-house. The region of Jyväskylä has been designated by the Finnish government as a cybersecurity centre; the presence of the University of Jyväskylä provides clear advantages to the defence forces.

Norway has a Defence Cyber Academy, providing a Bachelor's degree after three years of study, and cyber technician training. Diplomas are not the only criterion for recruitment: conscripts with the right skillset are also sought after. Creativity is considered more important: self-taught skills and outside-the-box thinking are what the Armed Forces look for.

The vision of the Swedish Armed Forces regarding cyber conscription states that in 2023 this training programme will be considered the most advanced cybersecurity education in Sweden, that the number of applicants will exceed the number of positions, and that conscripts will be proud of having been selected and appreciate the skills and competence of the instructors. The planned number of cyber conscripts to be trained is 30 in 2020, 45 in 2021 and 60 in 2022; the longer-term aim, beyond 2023, is to increase the number further.

Swedish cyber conscripts receive specialist training over 22 weeks, during which KTH Royal Institute of Technology plays an important role

Swedish cyber conscripts undertake a ten-week basic military training package similar to other conscripts. For the latter, this basic military training course lasts for 12 weeks but this package has been shortened for cyber conscripts to enable a greater focus on specialist training. Second, cyber conscripts receive specialist training over 22 weeks, during which KTH Royal Institute of Technology plays an important role. KTH has a Centre for Cyber Defense and Information Security (CDIS) that is responsible for providing courses to soldiers. These courses aim to increase the soldiers' understanding of computers and networks, security (both in general and in information technology), log and network analysis, ethical hacking and cyber ethics. The CDIS employs six Ph.D researchers who will deliver the courses at the Command and Control Regiment in Enköping. Individual studies are important, although there is also a lot of emphasis on the team aspect, something that is reflected in the small-scale accommodation of cyber conscripts that stands in stark contrast to more traditional military lodging of entire companies on each floor. In addition, private cybersecurity companies will provide two practical courses on specific tools. The Armed Forces will also train the conscripts on topics related to military security to raise their awareness of today's threats. Third, during the final six-week-long block, conscripts will undergo unit-level training on their future positions aimed at applying the theory in practice. This can take place as on-the-job learning at the Swedish Armed Forces Communication and Information Systems Command (SwAF CISCOM), located in Örebro, or in Swedish Air Force C2 elements, where the individuals will be assigned to wartime positions upon completion of their conscript training.

Training for cyber conscripts in Switzerland includes about 800 hours of lectures and exercises in the cyber domain. They finish their basic training with the rank of sergeant. The 800 hours are credited, either towards a federal diploma or as points towards a degree. The overall duration of their military service is 440 days: 40 weeks of basic training (compared to the more common length of 18 weeks) and about 22 weeks as part of the annual four-week refresher courses. After basic military training, most cyber conscripts go to university and study in cyber-related fields. This leads to constant improvement in theoretical cyber-knowledge from one refresher course to the next. At this point, the conscripts are tasked to support the professionals according to their specific cyber-skills.

In August 2018, the Swiss Armed Forces' first 18 cyber conscripts started the new cyber course.[56] The Swiss Armed Forces currently train around 20 cyber conscripts in each of two cycles a year. The number of conscripts per cycle is planned to double.

[56] Sandra Christen and Nick Mäder, "So schult die Armee in der Cyber Rekrutenschule ihre Hacker" [This is how the Army trains its hackers at the Cyber Recruit School], *Nau.ch*, 21 September 2018, https://www.nau.ch/news/schweiz/so-schult-die-armee-in-der-cyber-rekrutenschule-ihre-hacker-65426539.

B.4. Service

In Estonia, the specific duties of a person during conscription are very much based on the result of previous profiling and the type of service the individual has been selected for. As a general principle, cyber conscription consists of a significant proportion of actual service and less training or formal courses. Originally, conscripts were used to support the helpdesk and later they were also employed in the Computer Incident Response Capability (CIRC) and for development. Today Estonian cyber conscripts fulfil ICT-related tasks including programming and development and they also support stratcom and the CIRC by assisting full-time military and civilian employees.

In Finland, cyber conscripts fulfil the functions of network protection, infrastructure architecture designers and coders, network intelligence, and offensive capabilities

In Finland, cyber conscripts fulfil the functions of network protection (defensive tasks), infrastructure architecture designers and coders (according to unit requirements), network intelligence (allowed by law since 2018), and offensive capabilities (gradually).

In Norway, conscripts serve as operations room assistants.

In Denmark, conscripts are given general awareness about securing networks and how to behave in social media, and work with common networks and databases.

The cyber-defence organisation in Finland is currently larger than company-strength equivalent and consists of both full-time professionals and reservists. Its task is to defend military networks. Cyber conscripts serve as operators who monitor networks or work in maintaining the Finnish Defence Forces cyber range. They are treated as individuals and often work 0900–1700 as full-time employees of the Finnish Defence Forces. Some of the networks with which conscripts work are classified, but most are not.

In Switzerland, cyber conscripts are deployed to support one of three Armed Forces cyber specialist teams: the Military Computer Emergency Response Team (milCERT), the CNO team and the Cyber Defence (CYD) team.

B.5. Reserve

Denmark has no concrete plans for cyber reserves and individuals who have finished cyber conscription will be instead assigned to a specific reserve pool. One possibility is to call up reservists to participate in certain exercises and to offer complementary training to keep them up to date.

In Estonia, following conscription service, a soldier is assigned to a position in the reserve. Cyber reservists may be called up for short refresher training, especially in the first few years after the end of their conscription. This training usually focuses on basic military and cyber skills (e.g. EDF IT systems), as there is not enough time to learn new advanced skills.

In addition to the EDF, Estonia has a voluntary national defence organisation, the Estonian Defence League (EDL), which operates under the Ministry of Defence and is part of the national military chain of command. The EDL Cyber Defence Unit (CDU) is both a potential source of cyber conscripts (identifying and recommending suitable candidates) and an alternative for those cyber reservists who prefer to perform a more active reserve service. Compared to standard reserve service, members of the EDL CDU regularly participate in cybersecurity training and

In Finland, cyber reservists staff wartime positions in strategic- and operational-level headquarters

exercises and can support the military (Cyber Command) or civilian authorities across the full spectrum of crises.[57]

The Finnish Defence Forces have used cyber reservists since the 1990s (when the term "computer network warfare" was used rather than "cyber"). Reservists are hand-picked and must be recommended by two other people. During refresher training they work more with classified live systems than conscripts do due to their higher level of experience. Cyber reservists staff wartime positions in strategic- and operational-level headquarters. It is believed that, from 2021 at the earliest, expansion will take place and cyber reservists will also fill positions at the tactical level, albeit with less-technical tasks.

In Norway, a recent study concluded that it will be possible to assign most youngsters who have received good cybersecurity training to the Norwegian Home Guard (*Heimevernet*) and earmark them for digital readiness. The Armed Forces should consider establishing a dedicated national readiness unit for cyber defence, for example in the Home Guard and with personnel who maintain the relevant level of competence.[58]

Although all Swedish cyber conscripts will be assigned to reserve positions, a small number may be recruited to the Armed Forces as civilian or military personnel. Nevertheless, the intention is that the trained conscripts will increase the skills of society in general and maintain their skills while working for the private sector or other organisations.

Swiss cyber NCOs are required to complete 440 days of service, of which about 280 are taken up with basic military and leadership training, while officers (OF-1) are required to complete 680 days' service. Once the cyber conscripts have completed their basic military and leadership training, they return to the Armed Forces for annual refresher training, usually of three weeks' duration (19 days). Swiss reservists attend military refresher training every year until they achieve the requisite number of days. They then do not need to complete further refresher training but can be called upon in cases of emergency until 12 years after their basic military training (around when they turn 30 for NCOs and until the age of 40 for officers (OF-1)).[59]

[57] The first cyber-defence units were *de facto* formed within the volunteer EDL in 2009. In January 2011, the CDU was formally established. Its primary objectives are to develop a reserve of experts and a cooperation network, including for crisis response; to promote awareness, education and training in the field of information security; to improve the security of civilian critical information infrastructure; and to improve the security of military ICT systems.

[58] Svendsen et al., *Økt evne til å kombinere menneske og teknologi*, 87.

[59] Baezner, "Study on the Use of Reserve Forces in Military Cybersecurity."

ANNEX C. LIST OF REFERENCES

Aregger, Alexandra, and Oliver Borner. "Schweizer Armee hat ihre ersten Cyber Rekruten ausgebildet" [The Swiss Army has trained its first conscripts]. *Nau.ch*, 26 May 2019. https://www.nau.ch/news/videos/schweizer-armee-hat-ihre-ersten-cyber-rekruten-ausgebildet-65526664.

Baezner, Marie. "Study on the Use of Reserve Forces in Military Cybersecurity." Center for Security Studies (CSS), ETH Zürich, 2020. https://doi.org/10.3929/ethz-b-000413590.

Bigelow, Brad. "What are Military Cyberspace Operations Other Than War?." In *2019 11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga and G. Visky. Tallinn: NATO CCD COE Publications, 2019. https://ccdcoe.org/uploads/2019/06/Art_10_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf.

Center for Cybersikkerhed (Centre for Cyber Security) (Denmark). "Nysgerrige cyberværnepligtige besøgte CFCS" (Curious cyber conscripts visited CFCS), 2 November 2020. https://cfcs.dk/da/nyheder/2020/nysgerrige-cybervarnepligtige-besogte-cfcs/.

Christen, Sandra, and Nick Mäder. "So schult die Armee in der Cyber Rekrutenschule ihre Hacker" [This is how the Army trains its hackers at the Cyber Recruit School]. *Nau.ch*, 21 September 2018. https://www.nau.ch/news/schweiz/so-schult-die-armee-in-der-cyber-rekrutenschule-ihre-hacker-65426539.

Disobey. "Disobey postponed to 2022." Last accessed 28 January 2021. https://disobey.fi/2021/.

Fadum, Elin Anita, Einar Kristian Borud, and Leif Aage Strand. "The Norwegian Armed Forces Health Registry and use of military screening data to evaluate changes in IQ scores over time." *Revue d'Épidémiologie et de Santé Publique* (Journal of Epidemiology and Public Health), Vol. 66, Supplement 5 (2018), S343. https://www.sciencedirect.com/science/article/abs/pii/S0398762018309878.

Federal Council (Switzerland). "Federal Constitution of the Swiss Confederation. Art. 58–59." https://www.admin.ch/opc/en/classified-compilation/19995395/index.html.

Federal Council (Switzerland). *National Strategy for the Protection of Switzerland Against Cyber Risks (NCS) 2018–2022*. Bern: Federal IT Steering Unit, April 2018. https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.

Finnish Defence Forces. "Call-ups." Conscript Webpage. Accessed 20 October 2020. https://intti.fi/en/call-ups.

Finnish Defence Forces. "Conscription - a Finnish choice." Conscription. Accessed 20 October 2020. https://puolustusvoimat.fi/en/finnish-conscription-system.

Forsvaret (Danish Defence). "Cyberværnepligt" [Cyber conscription]. Accessed 10 November 2020.https://karriere.forsvaret.dk/varnepligt/varnepligten/cybervarnepligt/.

Forsvaret (Danish Defence). "Efter Forsvarets Dag" [After Defence Day]. Accessed 10 November 2020. https://karriere.forsvaret.dk/varnepligt/forsvaretsdag/efter/.

Forsvaret (Danish Defence). "Forsvarets Dag" [Defence Day]. Accessed 10 November 2020. https://karriere.forsvaret.dk/varnepligt/forsvaretsdag/.

Forsvaret (Norwegian Armed Forces). "Egen-erklæring" [Self-declaration]. Accessed 3 November 2020. https://www.forsvaret.no/egenerklaering.

Forsvaret (Norwegian Armed Forces). "Sesjon" (Examination). Accessed 3 November 2020. https://www.forsvaret.no/sesjon.

Forsvaret (Norwegian Armed Forces). "Verneplikt" [Conscription]. Accessed 3 November 2020. https://forsvaret.no/forstegangstjeneste/verneplikt.

Försvarsmakten (Swedish Armed Forces). "Första kullen cybersoldater redo att rycka in" [First cyber conscripts ready to be called up]. 18 May 2020. https://www.forsvarsmakten.se/sv/aktuellt/2020/05/forsta-kullen-cybersoldater-redo-att-rycka-in/.

Försvarsmakten (Swedish Armed Forces), "Grundutbildning med värnplikt" [Basic military training under conscription]. Accessed 27 October 2020. https://jobb.forsvarsmakten.se/sv/ordlista/#/word/militar-grundutbildning.

Forsvarsministeriet (Ministry of Defence) (Denmark). "Defence Agreement 2018–2023". https://fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2018-2023-pdfa-2018.pdf.

Huhtanen, Jarmo. "'Se on nyt modernimpi psykologisia käsitteitä mittaava testi" – Armeija uusii varusmiesten 'palikkatestit', nämä viisi väitettä karsiutuivat lopullisesta versiosta" ["It is now a more modern test measuring psychological concepts" – Army renews conscript "block tests", these five claims were eliminated from the final version]. *Satakunnan Kansa*, 8 May 2020. https://www.satakunnankansa.fi/a/0c279474-8446-4540-9673-7d47adca85ae.

Jaakson, Tiina. "Klassikaupa ajateenistusse minek on üha populaarsem" [School classes undergoing conscription together increasingly popular]. *ERR*, 13 July 2020. https://www.err.ee/1112450/klassikaupa-ajateenistusse-minek-on-uha-populaarsem.

Kaitseministeerium (Ministry of Defence) (Estonia). *Aruanne kaitseväekohustuse täitmisest ja kaitseväeteenistuse korraldamisest 2019. aastal* [Report on the Fulfilment of Military Service and on the Organisation of Conscription in 2019]. Tallinn: Kaitseministeerium, 2020. https://www.kra.ee/static/aruanne_kaitsevaekohustuse_taitmisest_riigis_2019.pdf.

Kaitseressursside Amet (Defence Resources Agency) (Estonia). "Arstlik komisjon" [Medical board]. Last modified 31 December 2020 https://kra.ee/arstlik-komisjon/.

Kaitseressursside Amet (Defence Resources Agency) (Estonia). "Kõrgharidus ja ajateenistus" [Higher education and conscription]. Last modified 27 August 2020. https://kra.ee/ajateenistus/ajateenistusest/korgharidus-ja-ajateenistus/.

Korhonen, Tiia. "Puolustusvoimien 'pällitestin' kysymykset huvittavat – mistä kokeessa on oikeasti kysymys?" [The questions in the "top test" of the Defence Forces are amusing - what is really the question?]. *Yle*, 29 August 2017. https://yle.fi/uutiset/3-9798024.

Laikoja, Linda-Liis. "'Kübersõdur' on sõna, mis kõlab nagu terminaatorlik tegelane kuskilt ulmefilmist, kuid mille taga tegelikult peitub meie riigi turvalisus" ["Cyber soldier" is a word that sounds like a Terminator-like character from a science-fiction movie while in fact protecting our state]. *DigiPRO*, 17 December 2020. https://digipro.geenius.ee/eksklusiiv/paev-kubersoduri-elus-on-nagu-startupis-tootamine/.

Ministry of Defence (Estonia). "Estonian Military Defence 2026." https://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/rkak2026-a6-spreads_eng-v6.pdf.

North Atlantic Treaty Organization. "Cyber defence." Topics. Last modified 25 September 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Norwegian Armed Forces. "Norwegian Cyber Defence." Organisation. Last modified 11 October 2020. https://www.forsvaret.no/en/organisation/norwegian-cyber-defence.

Pernik, Piret. *Preparing for Cyber Conflict: Case Studies of Cyber Command*. Tallinn: International Centre for Defence and Security, 2018. http://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

Põltsamaa Ühisgümnaasium (Põltsamaa Secondary School). "Infotehnoloogia (IT)- ja küberkaitse õppesuund" (Information Technology (IT) and cyber defence specialisation). Last modified 17 March 2020. https://www.poltsamaa.edu.ee/en/node/468.

Prime Minister's Office (Finland). *Government's Defence Report*. Helsinki: Prime Minister's Office Publications, 7/2017. https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf.

Regeringskansliet (Government Offices) (Sweden). "Regeringens proposition 2020/21:30. Totalförsvaret 2021–2025" [Government Bill 2020/21:30. Total Defence 2021–2025]. Stockholm, 14 October 2020. https://www.regeringen.se/4a965d/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsproposition-2021-2025/totalforsvaret-2021-2025-prop.-20202130.pdf.

Rekryteringsmyndigheten (Swedish Defence Recruitment Agency). "Mönstringsunderlag" [Basic information for mustering]. Last modified 6 February 2021.https://www.pliktverket.se/totalforsvarsplikten/monstring-och-monstringsunderlaget/monstringsunderlaget.

Rinne, Antti. *Hallituksen esitys eduskunnalle valtion talousarvioksi vuodelle 2020* [Government Proposal to Parliament for State Budget of 2020]. Helsinki: Edita Prima Oy, 2019. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_29+2019.pdf.

Schweizer Armee (Swiss Army). „Bereit für die Rekrutierung?" [Ready for recruitment?]. Accessed 30 November 2020. https://www.vtg.admin.ch/de/mein-militaerdienst/stellungspflichtige/rekrutierung.html.

Schweizer Armee (Swiss Army). "Dienstpflicht" [Obligation to serve]. Accessed 30 November 2020. https://www.vtg.admin.ch/de/mein-militaerdienst/allgemeines-zum-militaerdienst/dienstpflicht.html.

Schweizer Armee (Swiss Army). "Mein Orientierungstag" [My orientation day]. Accessed 30 November 2020. https://www.vtg.admin.ch/de/mein-militaerdienst/stellungspflichtige/orientierungstag.html#ui-collapse-502.

Svendsen, Berit, Øystein Bakken, Christian Chramer, Terje Hanssen, Solveig Hellebust, Kathleen Offman Mathisen, and Marit Warncke, *Økt evne til å kombinere menneske og teknologi. Veier mot et høyteknologisk forsvar* [Increased Ability to Combine Humans and Technology. Roads to a High-Tech Defence]. Oslo: Svendsen-utvalget, 2020. https://www.regjeringen.no/contentassets/374492dfae2f41a18f9b01e8678b468a/svendsen-utvalget--okt-evne-til-a-kombinere-menneske-og-teknologi.pdf.

Swedish Armed Forces. "Cyber Defence." Organisation. Accessed 27 October 2020. https://www.forsvarsmakten.se/en/about/organisation/cyber-defence/.

Swedish Defence Recruitment Agency. "A duty not reserved for everyone." https://www.rekryteringsmyndigheten.se/globalassets/dokument/varnplikt/2020/191209_en_rek_trycksak_a5_aw.pdf.

Sõmer, Tiia, Birgy Lorenz, and Rain Ottis, "Developing Military Cyber Workforce in a Conscript Armed Forces: Recruitment, Challenges and Options". In *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019),* edited by Noelle van der Waag-Cowling and Louise Leenen. Reading, UK: Academic Conference and Publishing International, 2020.

swissinfo.ch. "Apprenticeship system." Last modified 19 February 2019. https://www.swissinfo.ch/eng/apprenticeship-system/43796482.

Szymański, Piotr. "Overstretched? Denmark's security policy and armed forces in light of the new Defence Agreement." OSW Commentary no. 266, 20 April 2018. http://aei.pitt.edu/93810/1/commentary_266.pdf.

Vabariigi Valitsus (Government of the Republic) (Estonia). "Gümnaasiumi riiklik õppekava 2011" [State curriculum for secondary schools 2011]. *Riigi Teataja* (Estonian State Gazette), RT I, 14 January 2011, 2. https://www.riigiteataja.ee/akt/128072020013?leiaKehtiv.

RECENT ICDS PUBLICATIONS

REPORTS

Juurvee, Ivo, and Mariita Mattiisen. *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*. Tallinn: International Centre for Defence and Security, August 2020.

Sherr, James. *Nothing New Under the Sun? Continuity and Change in Russian Policy Towards Ukraine*. Tallinn: ICDS Estonian Foreign Policy Institute, July 2020.

Jermalavičius, Tomas, Priit Mändmaa, Emma Hakala, Tomas Janeliūnas, Juris Ozoliņš, and Krystian Kowalewski. *Winds of Change, or More of the Same? Impact of the 2018-19 Election Cycle on Energy Security and Climate Policies in the Baltic states, Poland and Finland*. Tallinn: International Centre for Defence and Security, May 2020.

Kacprzyk, Artur, and Łukasz Kulesa. *Dilemmas of Arms Control: Meeting the Interests of NATO's North-Eastern Flank*. Tallinn: International Centre for Defence and Security, April 2020.

Hodges, Ben, Tony Lawrence, and Ray Wojcik. *Until Something Moves: Reinforcing the Baltic Region in Crisis and War*. Tallinn: International Centre for Defence and Security, April 2020.

BOOKS

Raik, Kristi, and András Rácz (eds.). *Post-Crimea Shift in EU-Russia Relations: From Fostering Interdependence to Managing Vulnerabilities*. Tallinn: ICDS Estonian Foreign Policy Institute, 2019.

POLICY PAPERS

Loik, Ramon. "Volunteers in Estonia's Security Sector: Opportunities for Enhancing Societal Resilience." ICDS Policy Paper, June 2020.

Baranowski, Michał, Linas Kojala, Toms Rostoks, and Kalev Stoicescu. Tony Lawrence (editor). "What Next for NATO? Views from the North-East Flank on Alliance Adaptation." ICDS Policy Paper, June 2020.

Brauss, Heinrich, Kalev Stoicescu, and Tony Lawrence. "Capability and Resolve: Deterrence, Security and Stability in the Baltic Region." ICDS Policy Paper, February 2020.

Raik, Kristi, and Josef Janning. "Estonia's Partners in the EU Coalition Machinery: Maximising Influence in the EU through Coalition-building." ICDS/EFPI Policy Paper, January 2020.

ANALYSES

Kuusik, Piret. "Under Pressure: Nordic-Baltic Cooperation During the COVID-19 Crisis." ICDS/EFPI Analysis, February 2021.

Teperik, Dmitri, and Oksana Iliuk. "The Universe of Resilience: From Physics of Materials Through Psychology to National Security." ICDS Analysis, January 2021.

Muzyka, Konrad, and Rukmani Gupta. "A Relationship of Convenience: Russian-Chinese Defence Cooperation." ICDS Analysis, November 2020.

Stoicescu, Kalev. "Stabilising the Sahel: The Role of International Military Operations." ICDS Analysis, July 2020.

Kuusik, Piret. "Through the Looking Glass: The Nordic-Baltic Region and the Changing Role of the United States." ICDS/EFPI Analysis, June 2020.

Raik, Kristi. "Estonia in the UN Security Council: The Importance and Limits of European Cooperation." ICDS/EFPI Analysis, April 2020.

All ICDS publications are available from https://icds.ee/category/publications/.


ICDS.Tallinn


@ICDS _ Tallinn


ICDS-Tallinn


www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-0529
ISBN 978-9949-7484-8-8 (print)
ISBN 978-9949-7484-9-5 (pdf)